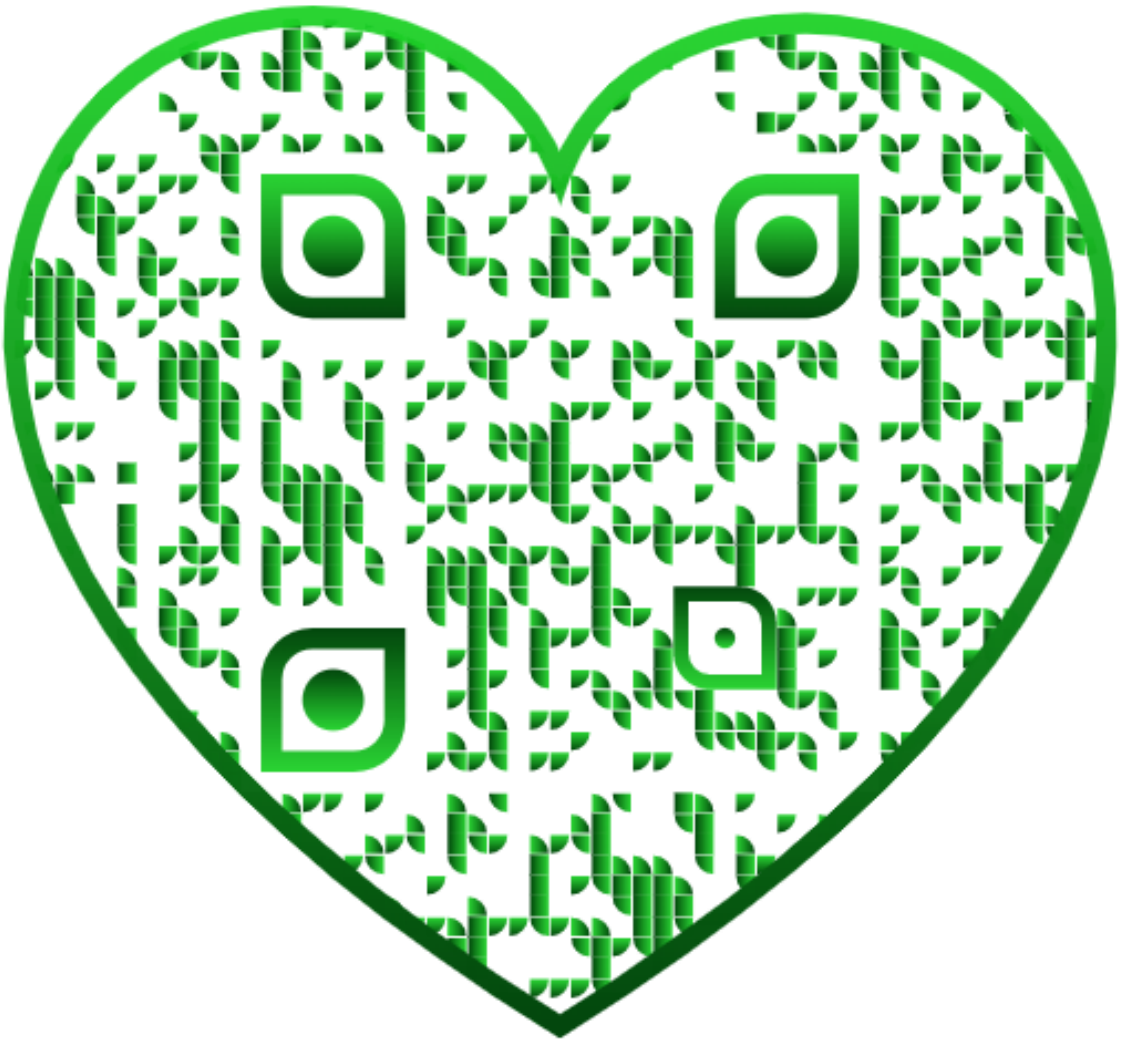
$\mathfrak{S}_6 \simeq \mathrm{Sp}_4(\mathbb{F}_2)$

Philippe Caldero
et Jérôme Germoni

Histoires hédonistes de groupes et de géométries

Tome second

Calvage & Mounet



MATHÉMATIQUES EN DEVENIR

Mathématiques en devenir

101. — Jacques Faraut. *Analyse sur les groupes de Lie. Une introduction*
102. — Patrice Tauvel. *Corps commutatifs et théorie de Galois*
103. — Jean Saint Raymond. *Topologie, calcul différentiel et variable complexe*
104. — Clément de Seguins Pazzis. *Invitation aux formes quadratiques*
105. — Bruno Ingrao. *Coniques projectives, affines et métriques*
106. — Wolfgang Bertram. *Calcul différentiel topologique élémentaire*
107. — Henri Lombardi & Claude Quitté. *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini*
108. — Frédéric Testard. *Analyse mathématique. La maîtrise de l'implicite*
109. — Grégory Berhuy. *Modules : théorie, pratique... et un peu d'arithmétique*
110. — Bernard Candelpergher. *Théorie des probabilités. Une introduction élémentaire*
111. — Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries. Tome premier*
112. — Gema-Maria Díaz-Toca, Henri Lombardi & Claude Quitté. *Modules sur les anneaux commutatifs*
113. — Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries. Tome second* – encores

Philippe Caldero et Jérôme Germoni

Histoires hédonistes de groupes et de géométries

Tome second – *encores*

Calvage & Mounet

PHILIPPE CALDERO est ancien élève de l'ÉNS de Saint-Cloud, agrégé de mathématiques et maître de conférences à l'université Lyon 1. Il y est responsable de la préparation à l'Agrégation interne. Ses travaux de recherche concernent la théorie des représentations.

JÉRÔME GERMONI est ancien élève de l'ÉNS, agrégé de mathématiques et maître de conférences à Lyon 1. Passionné de questions d'enseignement et de diffusion de la culture mathématique, il a dirigé jadis l'IREM de Lyon et dirige maintenant la Maison des mathématiques et de l'informatique de Lyon (MMI).

germoni@math.univ-lyon1.fr
caldero@math.univ-lyon1.fr

Mathematics Subject Classification (2000) :

14-XX Algebraic geometry
  14H-XX Curves
    14.20 Algebraic curves, surfaces and special varieties
51-XX Geometry
  51F-XX Metric geometry
  51N-XX Analytic and descriptive geometry
    51N10 Affine analytic geometry
    51N15 Projective analytic geometry
    51N20 Euclidean analytic geometry
    51N25 Analytic geometry with other transformation groups
    51N30 Geometry of classical groups
    51A05 General theory and projective geometries

ISBN 978-2-91-635243-5

∞ Imprimé sur papier permanent

© Calvage & Mounet, Paris, 2015

À ceux avec qui nous partageons ces plaisirs mathématiques : étudiants, collègues, amis, qui sont parfois un peu les mêmes...

Table des matières

I. Grassmanniennes et matrices échelonnées

1. Compléments sur le déterminant 2
2. Plongement de Plücker de la grassmannienne 7
3. Décomposition de Bruhat 20
4. Caractérisation algébrique des cellules de Schubert 31
5. BN-paire et algèbre de Hecke 35
A. Ordre de Bruhat 45
B. Présentation de Coxeter du groupe symétrique 55
C. Exercices 61

II. Réduction des endomorphismes

1. Semi-simplicité 78
2. Commutant 82
3. Désingularisation de Springer du cône nilpotent 88
A. Plaidoyer pour les modules 92
B. Exercices 102

III. Problèmes d'algèbre linéaire

1. Problèmes des N sous-espaces 113
2. Le théorème de Jordan-Kronecker 124
3. Problèmes de type sauvage 132
4. Carquois : introduction 134
5. Suites exactes et extensions 139
6. Espace des représentations 142
7. Lemme de Ringel et théorème de Gabriel 150
8. Retour au problème des N sous-espaces... et au-delà 157
A. Algèbre de chemins et représentations 165
B. Diagrammes de Dynkin finis et affines 176
C. Théorème du rang constant 180
D. Polynômes et topologie 183
E. Exercices 186

IV. Combinatoire algébrique

1. Formule du binôme quantique 195
2. Ordre des groupes orthogonaux sur un corps fini 201
3. Sous-espaces isotropes 206
4. Cardinal du cône nilpotent sur un corps fini 213
A. Exercices 216

V. Graphes et configurations

1. Configurations : exemples et définition 228
2. Configurations et conique nilpotente 232
3. Cas particulier : configuration de Desargues 241
4. Chaînes de Clifford 245
5. Coloriages 250
A. Tangentes à une conique 269
B. Conjugaison sur un corps fini 272
C. Petits arbres ternaires 282
D. Exercices 283

VI. *Encores* sur les groupes de Lie classiques et isomorphismes exceptionnels

1. Études du groupe symplectique 292
2. Correspondances de Klein 303
3. Grassmanniennes de signature donnée 312
A. Faisceaux et sous-groupes à un paramètre 326
B. Exercices 327

VII. Droite projective et birapport

1. Birapport et théorie de Galois 335
2. Plan hyperbolique 344
3. Un arbre pour les triplets pythagoriciens 360
4. Birapport et configurations finies 368
A. Trajectoires orthogonales 375
B. Exercices 376

VIII. *Encores* sur les coniques

1. Structure de groupe sur une conique 383
2. Coniques et théorie des invariants 394
A. Polynômes sur, polynômes en... 403
B. Exercices 406

IX. Sous-groupes finis de SO(3) et solides platoniciens

1. Rappels 410
2. Sous-groupes finis de SO(3) : signature 414
3. Existence et unicité des sous-groupes de signature donnée . . . 418
A. Exercices 427

X. Sous-groupes finis de $SO_3(\mathbb{R})$ et théorie des représentations

1. Tétraèdre régulier et cube 430
2. L'icosaèdre et son groupe de symétrie 433
A. Représentations et caractères 443
B. Caractères 453
C. « La somme des carrés » 465
D. Algèbre de groupe 472
E. Représentations sur un sous-corps 475
F. Exercices 483

XI. Correspondance de McKay : caractères des sous-groupes finis de $SU_2(\mathbb{C})$

1. Relèvement de $SO_3(\mathbb{R})$ à $SU_2(\mathbb{C})$ 508
2. Graphe de McKay 512
3. Groupes cycliques 514
4. Groupes binaires diédraux 515
5. Groupe binaire tétraédral 520
6. Groupe binaire octaédral 522
7. Groupe binaire icosaédral 525
8. Versant géométrique de la correspondance 529
9. Une ubiquité remarquable 533
10. Apologie de John McKay 537
A. Produits tensoriels 540
B. Éclatements 543
C. Exercices 547

XII. Épilogue : réalisation projective de $\mathfrak{A}_6$ et autres isomorphismes exceptionnels

1. Méthode naturelle 560
2. Méthode géométrique 562
3. La lettre de Galois 564

Bibliographie **571**
Index **579**

— Party on, Garth ?
— Party on, Wayne !
Penelope Spheeris, *Wayne's world*, 1992.

Avant-propos

Le présent volume est le tome second de nos « histoires hédonistes ». L'objectif de l'ouvrage est de motiver, de présenter, et d'emmener le lecteur dans une visite contemplative des interactions entre groupes et géométries.

• Dans le tome premier, on introduisait, *in vivo*, les notions de base :
– les actions de groupes,
– les groupes topologiques et leurs actions continues,
– les dégénérescences d'orbites,
– les groupes de Lie...
On s'aidait alors de ces outils efficaces pour prendre du recul sur le programme de licence (et plus !)[1] — algèbre linéaire, réduction, matrices échelonnées, étude des formes quadratiques, problèmes et figures de géométrie plane, etc. — et pour y découvrir une unité cachée, avec le légitime dessein d'en tirer le meilleur bénéfice. Cela n'empêchait pas, chemin faisant, de s'attarder sur des objets étrangement attrayants, tels le corps... des quaternions, la droite projective, les solides platoniciens, tout comme sur divers sujets où la combinatoire prend corps (fini !) dans la géométrie discrète.

•• Nous suivrons à peu près, dans ce second tome, le même canevas que dans le tome premier, en nous concentrant sur les nombreux thèmes pour lesquels les groupes jouent un rôle déterminant. On retrouvera ainsi l'étude des grassmanniennes, la réduction, les formes bilinéaires symétriques ou antisymétriques, la combinatoire algébrique, la droite projective, l'étude des coniques, les solides platoniciens, mais dans ce volume, l'objectif est d'accompagner le lecteur, sans rupture, vers une connaissance plus approfondie, plus actuelle, tout en suivant le fil d'Ariane offert par l'action de groupe.

L'uniformité des méthodes contribue à l'unité de l'ouvrage, mais celui-ci est aussi conçu pour être lu comme un recueil de nouvelles, indépendantes dans une large mesure — où les chapitres, et même souvent les sections entre chapitres, sont relativement autonomes.

[1] Comprendre les actions de groupes, c'est sortir au fond de la caverne de Platon !

Afin de suivre un schéma plus « narratif » au centre des chapitres, et de garder sans interruption le lecteur immergé dans les diverses histoires proposées, nous avons attaché en annexe les théories plus abstraites (théorie des représentations, compléments de calcul différentiel, présentations d'un groupe, ordre de Bruhat). L'idée est de mettre au cœur du livre des « aventures » où ces théories se retrouvent « en situation ». Toutefois, ces annexes ne se limitent pas à des florilèges de résultats. Le lecteur est guidé dans la théorie et les preuves restent complètes.

Pour les agrégatifs... En particulier, un nouvel outil sera, nous l'espérons, apprécié des agrégatifs : la théorie des représentations. Celle-ci est illustrée dans un premier temps par la construction des solides platoniciens, suivie d'une étude tous azimuts de ces solides allant jusqu'à la théorie de McKay. Nous avons, à cet effet, disposé en annexe des chapitres X et XI un ensemble exhaustif de résultats et de preuves.

Les agrégatifs se réjouiront sans doute également de quelques thèmes de développement propices pour l'oral : des compléments sur la réduction des endomorphismes (commutant, bicommutant, semi-simplicité, calculs de cardinaux sur corps fini), la décomposition de Bruhat, et quelques applications des formes quadratiques. Les résultats utiles à l'agrégation sont en général bien balisés.

Un certain nombre de résultats classiques sont proposés sous forme d'exercices, à monter (ou démonter) selon un procédé bien habituel chez les clients d'un célèbre concepteur en ameublement suédois... Beaucoup d'exercices, les plus essentiels notamment, sont accompagnés d'indications détaillées.

Morceaux de bravoure. En marge de l'agrégation, et plus près des confins de la recherche actuelle, on découvrira dans ce tome second quelques morceaux de bravoure.

- Tout d'abord, au chapitre I, une étude algébrique des grassmanniennes est abordée à l'aide des coordonnées de Plücker. On verra par la suite comment cette approche algébrique[2] permet de caractériser les dégénérescences d'orbites. Puis, nous en profiterons, en fin de chapitre, pour motiver le lecteur à poursuivre sa route vers le calcul de Schubert.
- On trouvera ultérieurement, et plus précisément au chapitre III, une introduction à la théorie des carquois de Peter Gabriel. Cette théorie peut être vue comme le point culminant de la réduction, généralisant par exemple la réduction des applications linéaires et des endomorphismes, lorsque plusieurs espaces et plusieurs morphismes sont en jeu. Motivée en début de chapitre par l'étude des configurations de sous-espaces, puis, indépendamment, par la classification de couples d'applications linéaires

[2]Il y a en fait deux approches complémentaires.

(théorème de Jordan-Kronecker), la théorie des représentations de carquois met en œuvre une somme impressionnante de moyens allant de l'action de groupes de Lie jusqu'à l'homologie des modules sur une algèbre de dimension finie, tout en passant par la géométrie différentielle. Nous avons tenté d'éviter au maximum les prérequis de géométrie algébrique que l'on rencontre habituellement dans cette littérature.

- Enfin, nous guiderons le lecteur, dans le chapitre XI, vers le camp de base de la féconde théorie de McKay. En suivant les traces de cet admirable explorateur d'analogies qu'est John McKay, on observera les similitudes entre la théorie des représentations des sous-groupes finis de $SU_2(\mathbb{C})$ et l'étude de certaines singularités quotient associées.

Pour les jeunes chercheurs. Une des vocations du tome second est de pourvoir quelques outils de la recherche actuelle, à l'intention d'un étudiant en master ou d'un professeur en classe supérieure. Pour ce faire, la difficulté a souvent été de contourner les obstacles qui rendent laborieux l'accès aux différents sujets traités. Par exemple, le produit tensoriel, irremplaçable en théorie des représentations, ne sera défini que matriciellement au détriment de sa canonicité. De même, nous avons évité au maximum l'utilisation de théorèmes de géométrie algébrique, ou d'homologie, qui auraient été trop fastidieux à introduire, même si le contexte s'y prêtait relativement souvent.

Voici pêle-mêle quelques exemples d'objets introduits dans ce volume qui permettront de mieux comprendre les avancées de la recherche en ce domaine : algèbre de Hecke, BN-paires, algèbres de Hall, relations de tresses, variétés de Schubert, représentations de carquois, ordre de Bruhat, diagrammes de Dynkin, fonctions de Schur, invariant modulaire, théorie des invariants, théorie de McKay...

Ces objets n'étant que des enveloppes vides s'ils ne s'accompagnent pas d'outils, nous armons le lecteur de techniques plus poussées ; citons, pêle-mêle, le tiré en arrière et poussé en avant, le plongement de Plücker, le pfaffien, les lagrangiens, la simplicité, la géométrie hyperbolique et le demi-plan de Poincaré, l'utilisation des groupes libres, présentations et algèbres de groupes, l'algèbre extérieure, les éclatements...

Nouveautés relatives. « ..., rien ne se crée, tout se transforme », a dit autrefois Antoine Lavoisier. Aussi trouvera-t-on donc dans ce tome second l'écho de quelques éléments de « culture orale », de conversations envolées, d'échanges furtifs sur des forums, de preuves sur un bord de tableau, effacées mais gravées désormais sur papier, à défaut de marbre. Bref, des histoires dont la paternité sera attribuée à l'air du temps et à la poussière de craie qu'il colporte. Parmi ces éléments, on rencontrera la réalisation de

la configuration de Desargues dans le plan projectif $\mathbb{P}^2(\mathbb{F}_5)$, point de départ de conversations, à la sauvette, entre les deux auteurs. On y découvrira quelques histoires du même acabit, moins connues, voire inédites :

- une dérivation de la formule du triple produit de Jacobi par dénombrement de sous-espaces vectoriels finis,
- une généralisation du point de Miquel,
- une incursion ludique et naturelle de la théorie de Galois dans la réalisation algébrique du birapport,
- une construction du plan de Fano $\mathbb{P}^2(\mathbb{F}_2)$ par des triangles équilatéraux de la droite projective $\mathbb{P}^1(\mathbb{F}_7)$,
- un calcul du cardinal du cône nilpotent sur un corps fini, par une méthode de type désingularisation,
- une structure d'arbre binaire sur les triplets pythagoriciens.

Parcours transverses. Qu'ils concernent les groupes finis ou les groupes de Lie, les isomorphismes exceptionnels sont les figures de proue de l'ouvrage. Ils ouvrent en fait des voies, ou disons des passerelles, entre divers points de vue, entre diverses géométries[3]. C'est pourquoi, dans un recueil d'histoires, apparemment indépendantes, mais reliées par des concepts communs, ces isomorphismes de groupes s'avèrent omniprésents.

On les rencontrera tout particulièrement dans le chapitre V, au moment de la réalisation des configurations, au chapitre VI avec les plongements de Segre, Véronèse et Plücker, via la théorie de Lie. Ils sont surtout compilés (notamment ceux qui concernent les groupes finis) dans le dernier chapitre, essai de synthèse autour du testament de Galois, donc au plus proche des considérations d'origine sur les groupes. Ils y feront le lien entre solides platoniciens (sur corps finis), combinatoire et formes quadratiques.

Cependant, un bon nombre d'autres objets mathématiques partageront cette ubiquité. Il ne faudrait pas attribuer cela au hasard, mais plutôt à la forte unité de la théorie, ou au signe de l'existence de liens, voire de correspondances, entre les différentes thématiques. En voici quelques-uns.

- On a parmi eux les actions de groupes, que l'on coudoie, par exemple, dans les problèmes de dénombrement, mais aussi, dans le cadre des actions continues de groupes topologiques, donnant lieu à des orbites localement fermées, et induisant un ordre naturel sur l'espace quotient, appelé ordre de dégénérescence. Ce schéma est présent dans la construction de l'ordre de Bruhat, pour les grassmanniennes, les variétés des drapeaux. On le retrouve également avec l'ordre de Chevalley sur les orbites nilpotentes, étonnamment dans le cadre des formules sur les coloriages. Cet ordre de Chevalley apparaît comme cas particulier de l'ordre de dégénérescence des orbites de carquois. D'ailleurs, tant pour l'ordre de Bruhat

[3]Pour paraphraser Tolkien, on dirait : "One group to rule them all!"

que pour l'ordre de Chevalley généralisé, nous constaterons que ces ordres de nature *a priori* topologique, possèdent une interprétation purement algébrique (variétés de Schubert pour l'un, ordre « ext » et « hom » pour l'autre).

- La grande star du livre reste évidemment le « pivot de Gauss », que l'on peut voir comme une méthode algorithmique de recherche de formes normales pour les orbites d'une action. La méthode du pivot est au rendez-vous dans la décomposition de Bruhat et s'adapte à la classification des grassmanniennes, des cellules de Schubert, mais aussi dans la détermination des classes de similitudes via une correspondance avec les $\mathbb{K}[X]$-modules. On la retrouve implicitement dans la combinatoire algébrique, en particulier, dans formule du binôme quantique, qui provient de la décomposition en cellules (B-orbites) de la grassmannienne sur un corps fini.
- Les solides platoniciens sont à l'honneur. Nous avons d'ailleurs pris le parti de les présenter comme un des leitmotiv les plus intrigants de l'histoire des mathématiques. Ils sont ominiprésents, bien sûr, lors de la classification des sous-groupes finis de $SO_3(\mathbb{R})$, mais aussi dans la théorie des représentations de ces groupes, dans la fascinante théorie de McKay. Pour le fun, on s'amusera à les colorier à l'aide du théorème de Pólya. Rappelons aussi que, lors du tome premier, ceux-ci ont joué un rôle déterminant pour la construction d'isomorphismes exceptionnels. Leurs avatars se révèlent même avec sur les corps finis, dans le chapitre XII, toujours dans le cadre de la construction d'isomorphismes exceptionnels, eux-mêmes liés aux questions originelles de Galois.
- En lien avec les solides platoniciens, on introduira les diagrammes de Dynkin (affine ou non). Sans raison apparente, ceux-ci interviennent à la fois en théorie des représentations de carquois, dans la classification des carquois de type fini et docile, ainsi que chez les sous-groupes finis de $SU_2(\mathbb{C})$ via la théorie des représentations[4]. On s'aperçoit des traces évidentes de leur présence lors des éclatements de singularités quotient de $\mathbb{C}^2$, et enfin dans l'étude des fonctions sous-additives sur les graphes.
- La classification des coniques (parabole, hyperbole, ellipse), étudiée au tome premier, n'est pas l'apanage des trajectoires orbitales... ou alors, dans un sens moins astronomique de la notion d'orbite. On retrouvera cette classification dans les chapitres V, VI et VII, en connexion avec la réduction de matrices de 2×2 de trace nulle, les sous-groupes à un paramètre de $PSL_2(\mathbb{R})$, et enfin avec les faisceaux de cercles. Pour finir, elle intervient au moment de la détermination des classes de conjugaison de groupes sur les corps fini, lorsque l'on cherche à « colorier » la droite projective.

[4]Ils sont aussi incontournables dans la théorie des algèbres de Lie semi-simples.

- Enfin, le birapport ne sera pas en reste, puisqu'on le rencontre au cœur des isomorphismes exceptionnels de groupes de petit cardinal (en exercice). Il sera le passeur vers la géométrie hyperbolique (et tous ses avatars). Il illustrera parfaitement la situation « affine » dans les représentations de carquois (le carquois de type affine $\tilde{D}_4$), sans oublier, bien sûr, son apport dans l'étude des cercles et droites, où il joue le rôle central d'invariant total pour l'action du groupe projectif $\mathrm{PGL}_2(\mathbb{C})$. Le birapport sera aussi un objet d'étude en soi, dans le cadre de la théorie de Galois, qui nous fera découvrir la forme modulaire qu'il recèle.

La transversalité ne s'arrête pas là. Symptômes flagrants de troubles obsessionnels compulsifs chez les deux auteurs, les inévitables preuves à répétition d'un même résultat à l'aide d'approches diverses s'éparpillent tout au long du tome second. On découvrira, par exemple, des preuves connues de Cayley-Hamilton (par densité, par les $\mathbb{K}[X]$-modules), le groupe simple $\mathrm{PSL}_2(\mathbb{F}_7)$ dans tous ses états (comme groupe simple à 168 éléments, via les BN-paires, agissant sur le plan de Fano), et l'automorphisme extérieur de $\mathfrak{S}_6$ (en lien avec les relations de tresses, avec la configuration de Cremona-Richmond, via divers isomorphismes exceptionnels).

Hommages. Ce livre offre une sorte de parcours qui mène de la fondation de l'algèbre moderne au camp de base de la recherche actuelle.

Nous y évoquerons le souvenir émouvant de la lettre testamentaire d'Évariste Galois : on découvre là, en germe, plusieurs problématiques qui n'ont cessé d'évoluer jusqu'à présent, qu'elles se situent au niveau de la compréhension d'objets mathématiques, de la structure adaptée à ces objets, ou au niveau de la construction de correspondances entre ces objets.

Notre chemin passera un grand nombre de fois dans le territoire défriché par le géomètre H.S.M. Coxeter, que ce soit dans ses travaux de recherche — la « présentation de Coxeter » des groupes symétriques est la porte d'entrée vers un immense domaine, qui voit converger presque tous les problèmes sur les groupes classiques — ou ses livres et articles de diffusion.

Toute notre considération va également à John McKay, qui, dans le même esprit, mais, cette fois-ci, à l'autre bout de la chaîne, a entrevu de nouvelles correspondances qui ont révolutionné ce domaine de la recherche.

Remerciements. Nous avons plaisir à remercier les étudiants qui se sont intéressés à notre travail, ont effectué des relectures minutieuses sur des points précis ou ont parfois, à travers leurs discussions, suggéré de jolis exercices. Nous citerons, parmi eux, Ahmed Al Hamar, Donatien Bénéat, Nicolas Chaigneau, Maxime Chatagnier, Jérémy Cochoy, Nicolas Doyen, Teddy Mignot, Marie Péronnier. Plusieurs collègues seront peut-être étonnés de se retrouver visés par ces remerciements ; pour certains sans le vouloir, ils nous ont été d'une aide précieuse, par leurs conversations, parfois

aussi pour des références, des idées d'exercices, et souvent pour leurs encouragements : Pierre Baumann, Cedric Bonnafé, Michael Bulois, Frédéric Chapoton, Michel Cretin, Paul Gérardin, Kenji Iohara, Bernhard Keller, Olivier Mathieu, Pierre Pansu, Serge Parmentier, Nicolas Ressayre, Alexis Tchoudjem, Amaury Thuillier, Nicolas Tosel, Jiang Zeng, sans oublier notre relecteur de choc Bruno Calado et notre *super-mentor* Rached Mneimné. Le cercle s'étend bien sûr aux non-mathématiciens qui ont su créer autour de nous une atmosphère inspiratrice, et sans qui ce livre n'aurait pas été ce qu'il est. Parmi eux, citons Monique Gaffier pour l'ambiance qu'elle a su instaurer au sein du labo et aussi Mireille et Joseph, qui ont été des hôtes particulièrement attentionnés pour le premier auteur. Nous aimerions au bout du compte saluer les mathématiciens qui nous ont influencés par leur travail et leur pédagogie : Michel Audin, Daniel Perrin et notre regretté collègue de la Northeastern, Andrei Zelevinsky.

Notre reconnaissance va, dernièrement et naturellement, aux jeunes éditions Calvage & Mounet pour le soin qu'elles ont apporté à l'élaboration du présent volume. Nous adressons en particulier le mot de la fin à Alberto Arabia, dont la maîtrise de LaTeX repousse les frontières du possible juste à côté de celles de l'imagination, et à qui nous sommes redevables des plus belles figures de l'ouvrage.

Signalisation

Nous avons dispersé ça et là quelques panneaux de signalisation. Certains parlent d'eux-mêmes,

d'autres nécessitent un décodage :

Danger classique.

Attention à rester dans le cadre des hypothèses. Une généralisation abusive pourrait être fatale.

Résultat de bon niveau qui peut s'exposer avec brio lors d'un oral de concours.

On dit qu'un sentiment de honte est vite passé, mais c'était avant Youtube. Évitez les peaux de banane !

Se munir d'un bon logiciel de calcul pour attaquer cette partie.

Concept plus métaphysique qui peut engendrer des désordres existentiels.

Les remarques et conseils éclairés (allumés ?) du Docteur Mabuse (Sischoen, de son prénom).

Réserve sauvage où le monde mathématique échappe à la raison humaine et sa soif de classification. Se munir de jumelles.

Les résultats doivent être manipulés avec soin par un professionnel. Don't try this at home !

Pourquoi ne pas faire une petite pause et admirer le paysage ?

Jeu très tendance consistant à prouver, en exercice, un résultat élémentaire à l'aide d'un théorème high-tech.

Alternative.

Résultat bien sympathique mais dont la preuve nous passera au-dessus de la tête. Pour ceux qui aiment prendre de l'altitude.

Une preuve qui roule pépère.

Si l'on change le manche, puis le fer d'une hache,
est-ce toujours la même hache ?
Adapté de David Wong, prologue de *John dies at the end*, 2007.

Chapitre I

Grassmanniennes et matrices échelonnées

À tout seigneur, tout honneur : le point de départ de ce chapitre est Carl Friedrich Gauss et son l'algorithme du pivot, que l'on exploite encore et encore. Mais si le maître semble s'effacer tout au long du chapitre, c'est pour laisser le relais à d'autres mathématiciens de premier plan comme Plücker, Grassmann, Ehresmann, Bruhat...

On fixe deux entiers naturels non nuls k et n et un corps $\mathbb{K}$. En ce qui concerne les constructions purement algébriques, le corps sera supposé quelconque, mais quand il s'agira de faire de la topologie, on supposera que $\mathbb{K}$ est le corps des réels ou des complexes.

Résumons le chapitre IV du tome premier. Là, la recherche d'une forme normale pour les matrices rectangulaires $n \times k$ modulo multiplication à droite par une matrice inversible conduit, grâce à l'algorithme de Gauss, à la notion de matrice échelonnée en colonnes (« co-échelonnées »). Géométriquement, cela donne une décomposition en « cellules » de la grassmannienne des k-plans dans $\mathbb{K}^n$ (si $k < n$...). En termes de groupes, c'est un paramétrage des orbites du groupe B des matrices triangulaires supérieures inversibles dans le quotient du groupe linéaire $G = \mathrm{GL}_n(\mathbb{K})$ par le sous-groupe « parabolique » P_k (redéfini ci-dessous). L'étude est complétée par la description de l'adhérence des cellules ou des B-orbites lorsque $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$.

Ici, on enrichit la situation de deux façons. D'abord, on munit la grassmannienne d'un système de coordonnées homogènes appelé *coordonnées de Plücker*. Il s'agit là de faire de la grassmannienne une variété algébrique projective en la plongeant dans un espace projectif : c'est le *plongement de*

Plücker. On trouve un système d'équations de son image, les *relations de Plücker.* C'est un long développement sur les déterminants, fondé sur les deux formules de la partie 1, qui ouvre les portes de la géométrie algébrique.

Ensuite, dans la partie 3 (p. 20), au lieu d'étudier l'ensemble des sous-espaces de dimension fixée, on étudie l'espace des drapeaux ; en termes de groupes, cela revient à étudier les B-orbites dans G/B. Cela donne lieu à la *décomposition de Bruhat*, qui est une extension (ou une version ?) de la décomposition LU d'une matrice. Cette partie n'est pas triviale, mais elle reste complètement élémentaire. Un cran plus loin, l'étude des adhérences des B-orbites dans l'espace des drapeaux met en évidence une interaction profonde entre la géométrie du groupe linéaire et la combinatoire du groupe symétrique (rappelée en annexe).

Un drapeau n'est qu'une suite finie de sous-espaces vectoriels emboîtés : dans la partie 4 (p. 31), on applique aux drapeaux les idées du plongement de Plücker pour obtenir une caractérisation algébrique des B-orbites des drapeaux et de leurs adhérences.

L'interaction entre géométrie et combinatoire est subsumée sous la notion de *BN-paire* ou *système de Tits*, utile également pour l'étude des autres groupes classiques. À titre d'application, on verra enfin un dernier avatar de la décomposition de Bruhat, incarnée dans l'algèbre d'Iwahori-Hecke, que l'on retrouvera à propos de représentations des groupes finis $\mathrm{GL}_n(\mathbb{F}_q)$, voir exercice X-F.21.

Dans ce chapitre, les intervalles tels que $[1, n]$ désignent des parties de $\mathbb{N}$.

1. Compléments sur le déterminant

On commence par montrer deux formules bien connues[1] sur le déterminant. D'abord, la *formule de Binet-Cauchy* généralise le caractère multiplicatif du déterminant à des matrices rectangulaires (de formats compatibles). Puis, la *formule de Laplace* étend le développement d'un déterminant par rapport à une rangée.

1.1. Notations. Pour n et r entiers naturels, on note $\Lambda(n, r)$ l'ensemble des parties de $[1, n]$ à r éléments. Ces parties seront chacune dotées d'un ordre fixé.

Pour m, n et r entiers, $I \in \Lambda(m, r)$ et $J \in \Lambda(n, r)$ et A est une matrice de taille $m \times n$, on note $\Delta_{I,J}(A)$ le mineur correspondant aux lignes indexées par I et colonnes indexées par J de A.

La *formule de Binet* ou *formule de Binet-Cauchy* peut s'énoncer ainsi.

[1] Après un bref sondage auprès d'algébristes et de combinatoriciens.

1.2. Théorème (Binet-Cauchy). *Soient k, ℓ, m, r des entiers naturels; $A \in \mathscr{M}_{k,\ell}(\mathbb{K})$ et $B \in \mathscr{M}_{\ell,m}(\mathbb{K})$. Alors, pour toutes parties I de $[1,k]$ et J de $[1,m]$ de même cardinal $|I| = |J| = r$, on a :*

$$\Delta_{I,J}(AB) = \sum_{K \subset [1,\ell], |K|=r} \Delta_{I,K}(A)\Delta_{K,J}(B).$$

Démonstration. Quitte à se restreindre à la sous-matrice de A constituée de ses lignes (indexées par) I et à la sous-matrice de B constituée de ses colonnes J, il suffit de montrer que si A et B sont respectivement de tailles $r \times \ell$ et $\ell \times r$, alors $\det(AB) = \sum_{K \in [1,\ell], |K|=r} \det(A_K)\det(B_K)$, où A_K (resp. B_K) est la sous-matrice de A (resp. de B) dont les colonnes (resp. les lignes) sont indexées par K.

Soient A_i $(1 \leqslant i \leqslant \ell)$ les colonnes de A; alors la j-ème colonne de AB est $\sum_{i=1}^{\ell} b_{i,j}A_i$ $(1 \leqslant j \leqslant r)$. En développant le déterminant grâce à la multilinéarité par rapport aux colonnes et à l'antisymétrie, on obtient :

$$\det(AB) = \sum_{K=\{i_1<i_2<\cdots<i_\ell\}} b_K \det(A_{i_1}, A_{i_2}, \ldots, A_{i_\ell}),$$

avec $b_K = \sum_{w \in \mathfrak{S}_K} \varepsilon(w) \prod_{k=1}^{r} b_{w(i_k),i_k}$. Cela donne la formule souhaitée. □

1.3. Exemple. Soient

$$A = \begin{pmatrix} 1 & -1 & 2 \\ -2 & 1 & -3 \end{pmatrix}, \quad B = \begin{pmatrix} -3 & 1 \\ 2 & -1 \\ 2 & 1 \end{pmatrix}, \quad AB = \begin{pmatrix} -1 & 4 \\ 2 & -6 \end{pmatrix},$$

$$\det(AB) = \begin{vmatrix} 1 & -1 \\ -2 & 1 \end{vmatrix}\begin{vmatrix} -3 & 1 \\ 2 & -1 \end{vmatrix} + \begin{vmatrix} -1 & 2 \\ 1 & -3 \end{vmatrix}\begin{vmatrix} 2 & -1 \\ 2 & 1 \end{vmatrix} + \begin{vmatrix} 1 & 2 \\ -2 & -3 \end{vmatrix}\begin{vmatrix} -3 & 1 \\ 2 & 1 \end{vmatrix}.$$

1.4. Remarques. La formule Binet-Cauchy généralise à la fois le produit matriciel (si $|I| = |J| = 1$) et, à l'autre extrême, la multiplicativité du déterminant (si les matrices sont carrées de taille n et $|I| = |J| = n$).

On obtient aussi comme corollaire que si $A \in \mathscr{M}_{m,n}(\mathbb{K})$, $B \in \mathscr{M}_{n,m}(\mathbb{K})$ avec $n < m$, alors $\det(AB) = 0$ (on applique la formule en sommant sur le vide). Mais ce résultat n'est pas étonnant puisque AB se factorise par A qui n'est pas surjective (et B qui n'est pas injective).

1.5. Remarque. Si $(v_1, \ldots, v_m)$ est une famille de vecteurs de $\mathbb{R}^n$, alors on sait (si l'on connaît les matrices de Gram) que le carré du volume[2] du parallélotope engendré par cette famille est égal à $\det(A\,{}^tA)$, où A désigne

[2]On suppose bien sûr que l'on a défini, de façon naturelle, le volume-unité dans le sous-espace de dimension m de l'espace euclidien $\mathbb{R}^n$.

la matrice (n,m) dont la j-ème colonne est donnée par v_j. La formule de Binet-Cauchy, pour $r=m$, dit alors que le carré du volume du parallélotope est égal à la somme des carrés des volumes des projections orthogonales sur les $\binom{n}{m}$ sous-espaces de coordonnées de dimension m. On obtient un théorème de Pythagore m-dimensionnel !

Le *développement de Laplace* ou *développement par blocs* qui suit est tout aussi naturel que la formule de Binet-Cauchy si l'on comprend bien le développement d'un déterminant par rapport à une ligne. On se donne une partie I de l'ensemble des lignes et on veut développer le déterminant d'une matrice par rapport aux lignes de I. Afin d'écrire la formule de façon simple, on introduit le nombre d'inversions d'une partie à une autre.

1.6. Définition. Soient I et J deux parties de $[1,n] \subset \mathbb{N}$. On définit le *nombre d'inversions*[3] de I à J par :

$$\iota(I,J) = |\{(i,j) \in I \times J,\ i > j\}|.$$

Pour I inclus dans $[1,n]$, on rappelle que l'on note $\bar{I}$ le complémentaire de I et $\ell(I) = \iota(I,\bar{I})$.

1.7. Lemme. *Soient I et J deux parties disjointes de $[1,n]$. Alors :*

$$\iota(I,J) + \iota(J,I) = |I|\,|J|.$$

Démonstration. Il suffit de remarquer que $I \times J$ est la réunion des deux ensembles qui apparaissent dans la définition de $\iota(I,J)$ et $\iota(J,I)$. □

1.8. Théorème (Développement de Laplace). *Soit A une matrice de $\mathscr{M}_n(\mathbb{K})$ et soit I une partie de $[1,n]$ de cardinal r. Alors :*

$$\det(A) = \sum_{J,|J|=r} (-1)^{\ell(I)+\ell(J)} \Delta_{I,J}(A)\Delta_{\bar{I},\bar{J}}(A).$$

Démonstration. On ordonne $I = \{i_1 < i_2 < \cdots < i_r\}$ et $\bar{I} = \{i_{r+1} < i_{r+2} < \cdots < i_n\}$, $J = \{j_1 < j_2 < \cdots < j_r\}$ et $\bar{J} = \{j_{r+1} < j_{r+2} < \cdots < j_n\}$. On notera w_I la permutation de $[1,n]$ qui envoie k sur i_k $(1 \leqslant k \leqslant r)$ et qui est strictement croissante sur $[1,n] \setminus \{1,\ldots,k\}$. Par définition de la signature, on a $\varepsilon(w_I) = (-1)^{\ell(I)}$.

On remarque que l'on peut factoriser $(-1)^{\ell(I)}$ dans le membre de droite de la formule de Laplace. Quitte à permuter les lignes par la permutation w_I et en utilisant sa signature, on peut se ramener au cas où $I = [1,r]$.

[3] C'est le nombre de transpositions qu'il faudra faire pour ordonner $I \cup J$.

Supposons donc $I = [1, r]$, de sorte que $\ell(I) = 0$. On note $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$. On a, d'une part,

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)},$$

et d'autre part, en notant $\mathfrak{S}_r = \mathfrak{S}([1, r])$ et $\mathfrak{S}_{n-r} = \mathfrak{S}([r+1, n])$:

$$\Delta_{I,J}(A) = \sum_{\sigma_r \in \mathfrak{S}_r} \varepsilon(\sigma_r) \prod_{i=1}^{r} a_{i,w_J \circ \sigma_r(i)},$$

$$\Delta_{\bar{I},\bar{J}}(A) = \sum_{\sigma_{n-r} \in \mathfrak{S}_{n-r}} \varepsilon(\sigma_{n-r}) \prod_{i=r+1}^{n} a_{i,w_J \circ \sigma_{n-r}(i)}.$$

Maintenant, à une permutation σ de $\mathfrak{S}_n$, on associe $I_\sigma = \sigma(I)$, $\sigma_r = w_{I_\sigma}^{-1} \sigma|_I \in \mathfrak{S}_r$ et $\sigma_{n-r} = w_{I_\sigma}^{-1} \sigma|_{\bar{I}} \in \mathfrak{S}_{n-r}$. On constate facilement que l'application $\sigma \mapsto (I_\sigma, \sigma_r, \sigma_{n-r})$ réalise une bijection de $\mathfrak{S}_n$ vers $\Lambda(r, n) \times \mathfrak{S}_r \times \mathfrak{S}_{n-r}$, où $\Lambda(r, n)$ désigne l'ensemble des parties à r éléments de $[1, n]$.

Soit $\sigma_n = (\sigma_r, \sigma_{n-r}) \in \mathfrak{S}_r \times \mathfrak{S}_{n-r}$ considérée de façon naturelle comme une permutation de $\mathfrak{S}_n$. On a $\varepsilon(\sigma_n) = \varepsilon(\sigma_r)\varepsilon(\sigma_{n-r})$. On note que la donnée de σ est équivalente à la donnée de $(\sigma_r, \sigma_{n-r}, I_\sigma)$, puisque $\sigma = w_{I_\sigma} \sigma_n$. Cela nous donne de plus l'égalité

$$\varepsilon(\sigma) = \varepsilon(w_{I_\sigma})\varepsilon(\sigma_n) = (-1)^{\ell(I_\sigma)} \varepsilon(\sigma_r)\varepsilon(\sigma_{n-r}).$$

Enfin, en multipliant les expressions de $\Delta_{I,J}(A)$ et de $\Delta_{\bar{I},\bar{J}}(A)$ dans la somme, on trouve :

$$\sum_{J:\ |J|=r} (-1)^{\ell(I)+\ell(J)} \Delta_{I,J}(A) \Delta_{\bar{I},\bar{J}}(A),$$

et en utilisant les formules obtenues, on obtient l'expression de $\det(A)$. □

1.9. Exemple. Le développement du déterminant d'une matrice arbitraire $A = (a_{i,j}) \in \mathscr{M}_4(\mathbb{K})$ par rapport aux lignes $I = \{1, 3\}$ donne :

$$\begin{aligned}
&- \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{3,1} & a_{3,2} \end{vmatrix} \begin{vmatrix} a_{2,3} & a_{2,4} \\ a_{4,3} & a_{4,4} \end{vmatrix} + \begin{vmatrix} a_{1,1} & a_{1,3} \\ a_{3,1} & a_{3,3} \end{vmatrix} \begin{vmatrix} a_{2,2} & a_{2,4} \\ a_{4,2} & a_{4,4} \end{vmatrix} - \begin{vmatrix} a_{1,1} & a_{1,4} \\ a_{3,1} & a_{3,4} \end{vmatrix} \begin{vmatrix} a_{2,2} & a_{2,3} \\ a_{4,2} & a_{4,3} \end{vmatrix} \\
&- \begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} \begin{vmatrix} a_{2,1} & a_{2,4} \\ a_{4,1} & a_{4,4} \end{vmatrix} + \begin{vmatrix} a_{1,2} & a_{1,4} \\ a_{3,2} & a_{3,4} \end{vmatrix} \begin{vmatrix} a_{2,1} & a_{2,3} \\ a_{4,1} & a_{4,3} \end{vmatrix} - \begin{vmatrix} a_{1,3} & a_{1,4} \\ a_{3,3} & a_{3,4} \end{vmatrix} \begin{vmatrix} a_{2,1} & a_{2,2} \\ a_{4,1} & a_{4,2} \end{vmatrix}
\end{aligned}$$

1.10. Puissances extérieures d'une matrice, représentations fondamentales de $\mathrm{GL}_n(\mathbb{K})$

Pour tout couple (r,n), on choisit[4] désormais un ordre total $\leqslant$ sur l'ensemble $\Lambda(r,n)$ des parties à r éléments de $[1,n]$. On associe à toute matrice A de $\mathscr{M}_{n,m}(\mathbb{K})$, et à $r \leqslant \max(n,m)$, la matrice

$$\Lambda^r(A) = \big(\Delta_{I,J}\big),\ I \in \Lambda(r,n),\ J \in \Lambda(r,m).$$

1.11. Exemples. Si A est une matrice $n \times r$, alors $\Lambda^r(A)$ est de taille $\binom{n}{r} \times 1$, c'est-à-dire un vecteur de $\mathbb{K}^{\Lambda(r,n)}$; si A est de taille $n \times n$, alors $\Lambda^r(A)$ est de taille $\binom{n}{r} \times \binom{n}{r}$, on l'identifie à un endomorphisme de $\mathbb{K}^{\Lambda(r,n)}$; si A est de taille $n \times n$ et $r = n$, alors $\Lambda^n(A) = \det(A)$.

La formule de Binet-Cauchy se récrit simplement :

$$\Lambda^r(AB) = \Lambda^r(A)\Lambda^r(B),$$

dès que les matrices A et B sont multipliables. On en tire deux conséquences utiles.

1.12. Corollaire. *Soient* $P \in \mathrm{GL}_n(\mathbb{K})$, $Q \in \mathrm{GL}_r(\mathbb{K})$, $A \in \mathscr{M}_{n,r}(\mathbb{K})$ *:*

$$\Lambda^r(PA) = \Lambda^r(P)\Lambda^r(A) \quad \textit{et} \quad \Lambda^r(AQ) = \det(Q)\Lambda^r(A).$$

1.13. Proposition. *Pour* $r \leqslant n$, *l'application* Λ^r *est un morphisme de groupes de* $\mathrm{GL}_n(\mathbb{K})$ *vers* $\mathrm{GL}(\mathbb{K}^{\Lambda(r,n)})$.

On définit ainsi une famille de *représentations linéaires* $(\Lambda^r)_{0\leqslant r\leqslant n}$ du groupe $\mathrm{GL}_n(\mathbb{K})$. On les appelle *représentations fondamentales* : sur le corps des complexes, elles permettent de construire toutes les représentations complexes dont les coefficients sont des fractions rationnelles des coefficients de la matrice.[5]

Pour $r = 0$, il s'agit de la représentation triviale ; pour $r = 1$, de la représentation standard, car Λ^1 est l'identité[6] de $\mathrm{GL}_n(\mathbb{K})$; pour $r = n$, on obtient la représentation déterminant

$$\Lambda^n = \det : \mathrm{GL}_n(\mathbb{K}) \longrightarrow \mathrm{GL}(\mathbb{K}^{\Lambda(n,n)}) \simeq \mathbb{K}^*.$$

Il est intéressant de reconnaître la représentation Λ^{n-1}. Il y a n parties à $n-1$ éléments si bien que $\mathrm{GL}_{\Lambda(n-1,n)}(\mathbb{K})$ est isomorphe à $\mathrm{GL}_n(\mathbb{K})$, et

[4] Même s'il y a des ordres naturels qui seraient de bons candidats, l'ordre choisi ici n'est pas réellement vital.

[5] Quitte à multiplier par une puissance du déterminant, on réalise toute représentation comme sous-représentation d'un produit tensoriel convenable, définie comme dans XI-A.3.

[6] Du moins, si l'on ordonne $\Lambda(n,1) = \{\{1\},\dots,\{n\}\}$ « comme » $[1,n] = \{1,\dots,n\}$.

on devrait voir apparaître un automorphisme de $\mathrm{GL}_n(\mathbb{K})$. De fait, si l'on ordonne les parties à n éléments selon l'ordre de l'unique élément manquant, *i.e.* $[1,n]\backslash\{i\} \leqslant [1,n]\backslash\{j\}$ si $i \leqslant j$, alors $\Lambda^{n-1}(A) = (m_{ij}(A))_{i,j}$, où $m_{ij}(A)$ est le mineur de A obtenu en effaçant la ligne i et la colonne j — le cofacteur d'indice (i,j). Si l'on note D la matrice diagonale $((-1)^{i-1})_{1\leqslant i\leqslant n}$, alors

$$\Lambda^{n-1}(A) = D\,\mathrm{com}(A)D^{-1},$$

où $\mathrm{com}(A)$ est la comatrice de A. Ainsi, la représentation Λ^{n-1} est isomorphe à la représentation « comatrice ». Au déterminant près, c'est la représentation duale de $\mathbb{K}^n$. Comme la comatrice s'écrit $P \mapsto \det(P)\,{}^tP^{-1}$, on reconnaît bien là un automorphisme (extérieur) de $\mathrm{GL}_n(\mathbb{K})$. Ces formules seront généralisées dans le §2.15 pour tout r compris entre 1 et n.

1.14. Exercice (Mineurs et polynôme caractéristique)

Soit n un entier non nul et soit A une matrice carrée de taille n.

1. *Montrer que si la matrice A a pour spectre $\{\lambda_1,\dots,\lambda_n\}$, alors $\Lambda^r(A)$ admet pour spectre $\{\lambda_{i_1}\cdots\lambda_{i_r},\ 1\leqslant i_1<\cdots<i_r\leqslant n\}$.*
2. *On note $\chi_A = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ le polynôme caractéristique de A. En déduire les relations :*

$$a_r = (-1)^{n-r}\,\mathrm{tr}\big(\Lambda^r(A)\big) = (-1)^{n-r}\sum_{I,|I|=r}\Delta_{I,I}(A).$$

1.15. Exercice. *Soit P_σ la matrice de permutation associée à la permutation σ de $\mathfrak{S}_n$,* i.e. *$P_\sigma = (\delta_{i,\sigma(j)})$, où δ désigne le symbole de Kronecker. Pour tout r dans $[1,n]$ et pour tout I de $\Lambda(r,n)$, on note ϕ_I l'unique fonction strictement croissante de $[1,r]$ vers I. Pour tout I, J dans $\Lambda^{(r,n)}$, soit $\varepsilon_{I,J}$ la signature de la permutation $\phi_I^{-1}\circ\sigma\circ\phi_J$ de $\mathfrak{S}_r$. Montrer que $\Lambda^r(P_\sigma)_{I,J} = \varepsilon_{I,J}\delta_{I,\sigma(J)}$, où δ est le symbole de Kronecker.*

Merci messieurs, c'était très bien. C'était très *bien.*

2. Plongement de Plücker de la grassmannienne

Faut reconnaître, c'est du brutal !
Michel Audiard, *Les Tontons flingueurs*, 1963.

Comment se représente-t-on, en son for intérieur, un sous-espace vectoriel ? Pour une droite vectorielle, on s'imagine une ligne droite. Pour un plan, disons un grand plateau. Et ensuite, on n'imagine plus grand chose au-delà

de l'espace ambiant. Grâce au plongement de Plücker, un sous-espace devient un point dans une variété (algébrique projective). Jusqu'à présent, on dispose seulement d'une topologie sur la grassmannienne de sous-espaces de dimension donnée d'un espace réel ou complexe, mais maintenant, non seulement nous travaillons dans un corps quelconque, mais la grassmannienne est promue au rang de variété algébrique projective, ce qui signifie en gros que nous pourrons la voir comme l'ensemble des points d'un espace, à un facteur scalaire près, dont les coordonnées, appelées coordonnées de Plücker, sont solutions d'un système d'équations polynomiales. En résumé, les grassmanniennes (réelles et complexes) ont été présentées comme des espaces topologiques avec action transitive d'un groupe (de Lie) ; maintenant, comme on dit, « y a mieux, mais c'est Plücker ».

Les grassmanniennes se voient donc ouverte la voie royale de la géométrie algébrique. Nous verrons que pouvons récupérer directement à partir des coordonnées de Plücker d'un sous-espace les coordonnées de son orthogonal et à partir des coordonnées de deux sous-espaces en position générique, les coordonnées de leur intersection. Encore une fois, la théorie des groupes n'est pas loin puisque nous rencontrerons chemin faisant des représentations du groupe linéaire.

2.1. Plongement de Plücker

Nous arrivons ici au cœur du problème : définir et décrire le *plongement de Plücker* $\psi = \psi_{r,n}$ de la grassmannienne $\mathrm{Gr}_{r,n}$ des sous-espaces vectoriels de dimension r de $\mathbb{K}^n$ dans l'espace projectif $\mathbb{P}\big(\mathbb{K}^{\Lambda(r,n)}\big)$ — voir [H2G2, II-D.2].

2.2. Proposition. *Soient r et n deux entiers avec $0 < r < n$.*

(i) *Soit F un sous-espace de dimension r de $\mathbb{K}^n$, et soit $A_F \in \mathscr{M}_{n,r}(\mathbb{K})$ la matrice d'une base de F dans la base canonique de $\mathbb{K}^n$. La droite engendrée par $\Lambda^r(A_F)$ ne dépend que de F. On note $[\Lambda^r(A_F)]$ le point correspondant dans l'espace projectif.*

On peut donc définir une application $\psi = \psi_{r,n}$ par

$$\psi : \mathrm{Gr}_{r,n} \to \mathbb{P}(\mathbb{K}^{\Lambda(r,n)}),\ F \mapsto [\Lambda^r(A_F)].$$

(ii) *L'application $\psi : \mathrm{Gr}_{r,n} \to \mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$ est injective.*

(iii) *L'application ψ commute avec les actions naturelles de $\mathrm{GL}_n(\mathbb{K})$. De plus, l'image de ψ est une orbite.*

(iv) *Si $\mathbb{K}$ est le corps des réels ou des complexes, l'application ψ est continue et l'image de ψ est compacte.*

Définition. Étant donnés r et n entiers avec $0 < r < n$, le *plongement de Plücker* est l'application $\psi = \psi_{r,n}$ définie dans la proposition 2.2.

Démonstration. (i) Par l'exemple 1.11, $\Lambda^r(A_F)$ est identifié à un vecteur de $\mathbb{K}^{\Lambda(r,n)}$, et ce vecteur n'est pas nul puisque A_F est de rang r ; on peut donc prendre sa classe dans l'espace projectif. Par ailleurs, soit A'_F la matrice d'une autre base de F. Si $Q \in \mathrm{GL}_r(\mathbb{K})$ désigne la matrice de passage, on a : $A'_F = A_F Q$, d'où : $\Lambda^r(A'_F) = \det(Q)\Lambda^r(A_F)$, par le corollaire 1.12. Ainsi, les droites engendrées par $\Lambda^r(A'_F)$ et $\Lambda^r(A_F)$ coïncident, si bien que l'application ψ est bien définie.

(ii) On va retrouver explicitement le sous-espace F à partir de son image $\psi(F)$, ce qui entraîne l'injectivité. Fixons une matrice A_F comme ci-dessus et soit $v \in \mathbb{K}^n$ un vecteur colonne. Alors, v appartient à F si et seulement si la matrice $B_v = (\, A_F \; v \,)$, déduite de A_F en ajoutant la colonne v, est de rang r. C'est-à-dire si et seulement si tout mineur de taille $r+1$ de B_v est nul. En développant ces mineurs par rapport à la colonne v, on obtient le système d'équations suivant :

$$\sum_{k=1}^{r+1} (-1)^k \Delta_{J\setminus\{j_k\}}(A_F) v_{j_k},$$

où $J = \{j_1, \ldots, j_{r+1}\}$ parcourt $\Lambda(r+1, n)$. Chaque équation étant homogène, le système ne dépend que de F et pas du choix de A_F, et il caractérise bien le sous-espace F à partir de son image $\big[\big(\Delta_J(A_F)_{J\in\Lambda(r,n)}\big)\big]$.

(iii) Le groupe $\mathrm{GL}_n(\mathbb{K})$ agit naturellement sur la grassmannienne par $P \cdot F = P(F)$ et sur $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$ par $P \cdot [v] = [\Lambda^r P(v)]$. La proposition 1.13 assure qu'il s'agit bien d'une action de groupes. Le corollaire 1.12 montre alors que ψ commute avec cette action : $\psi(P \cdot F) = P \cdot \psi(F)$, *i.e.* ψ est $\mathrm{GL}_n(\mathbb{K})$-équivariante. Comme l'action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathrm{Gr}_{r,n}$ est transitive, on déduit que l'image de ψ est une $\mathrm{GL}_n(\mathbb{K})$-orbite dans $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$. En particulier, si r vaut 1 ou n, alors ψ est bijective.

(iv) Sur $\mathbb{R}$ ou sur $\mathbb{C}$, l'application ψ est continue, voir exercice C.4. Comme la grassmannienne est compacte et l'espace projectif séparé (voir [H2G2, §II-D.2]), l'image de ψ est elle-même compacte. On peut d'ailleurs montrer que c'est la seule orbite compacte dans $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$. □

2.3. Exemple. Le plan F de $\mathbb{K}^4$ engendré par les deux vecteurs-colonnes ${}^t(a,b,c,d)$ et ${}^t(a',b',c',d')$ vérifie

$$\psi(F) = \left(\begin{vmatrix} a & a' \\ b & b' \end{vmatrix} : \begin{vmatrix} a & a' \\ c & c' \end{vmatrix} : \begin{vmatrix} a & a' \\ d & d' \end{vmatrix} : \begin{vmatrix} b & b' \\ c & c' \end{vmatrix} : \begin{vmatrix} b & b' \\ d & d' \end{vmatrix} : \begin{vmatrix} c & c' \\ d & d' \end{vmatrix} \right),$$

où l'ordre sur $\Lambda(2,4)$ est :

$$\{1,2\} < \{1,3\} < \{1,4\} < \{2,3\} < \{2,4\} < \{3,4\}.$$

2.4. Relations de Plücker

Les *relations de Plücker* sont des équations polynomiales homogènes de l'image de ψ : elles permettent de décider si un point de $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$ représente ou non un sous-espace de dimension r de $\mathbb{K}^n$.

2.5. Définition. Fixons $1 < r < n$. Pour tout I dans $\Lambda(r-1,n)$ et J dans $\Lambda(r+1,n)$, on définit la fonction polynomiale sur $\mathscr{M}_{n,r}(\mathbb{K})$:

$$\mathscr{P}_{I,J}(A) = \sum_{j,j\in J\setminus I} (-1)^{\iota(J\setminus j,j)+\iota(j,I)} \Delta_{I\cup\{j\}}(A)\Delta_{J\setminus\{j\}}(A),$$

où ι a été défini en 1.6.

Les *relations de Plücker* sont les relations : $\mathscr{P}_{I,J} = 0$.

Dans la pratique, on préférera la formule suivante, qui lui est équivalente. Si l'on ordonne $J = \{j_1 < j_2 < \cdots < j_{r+1}\}$, alors :

$$\mathscr{P}_{I,J}(A) = \sum_{k,j_k\notin I} (-1)^{k+\iota(I,j_k)} \Delta_{I\cup\{j_k\}}(A)\Delta_{J\setminus\{j_k\}}(A).$$

Puisque les mineurs en présence sont de taille r, on voit que $\mathscr{P}_{I,J}(A)$ est un polynôme quadratique en les coordonnées du vecteur $\Lambda^r(A)$.

2.6. Exemple. On rencontre la première relation non triviale dans $\mathrm{Gr}_{2,4}$:
- si $I = \{1\}$ et $J = \{2,3,4\}$, on a : $\mathscr{P}_{I,J} = -\Delta_{12}\Delta_{34} + \Delta_{13}\Delta_{24} - \Delta_{14}\Delta_{23}$;
- si $I = \{2\}$ et $J = \{1,3,4\}$, on a : $\mathscr{P}_{I,J} = \Delta_{12}\Delta_{34} + \Delta_{23}\Delta_{14} - \Delta_{24}\Delta_{13}$;
- si $I = \{1\}$ et $J = \{1,2,3\}$, on a : $\mathscr{P}_{I,J} = \Delta_{12}\Delta_{13} - \Delta_{13}\Delta_{12}$=0.

En fin de compte, toutes les relations de Plücker se résument en une seule, que l'on vérifie facilement pour toute matrice de $\mathscr{M}_{4,2}(\mathbb{K})$:

$$\Delta_{12}\Delta_{34} - \Delta_{13}\Delta_{24} + \Delta_{14}\Delta_{23} = 0.$$

2.7. Exercice. *Montrer que les relations de Plücker pour la grassmannienne* $\mathrm{Gr}_{2,n}$ *sont les* $\binom{n}{4}$ *relations décrites pour chaque quadruplet* $1 \leqslant i_1 < i_2 < i_3 < i_4 \leqslant n$ *par :*

$$\Delta_{i_1i_3}\Delta_{i_2i_4} = \Delta_{i_1i_2}\Delta_{i_3i_4} + \Delta_{i_2i_3}\Delta_{i_1i_4}.$$

Dans certains cercles (de mathématiciens !), on les appelle aussi relations de Ptolémée, *par analogie avec la formule sur les quadrilatères inscriptibles, voir figure 2.1 (cf. [H2G2, exercice X-C.8]).*

2.8. Remarque (Coordonnées homogènes et annulation d'un polynôme). Soit N un entier naturel non nul et soit p un point de $\mathbb{P}(\mathbb{K}^N)$, c'est-à-dire une droite de $\mathbb{K}^N$. Les *coordonnées homogènes* de p sont la

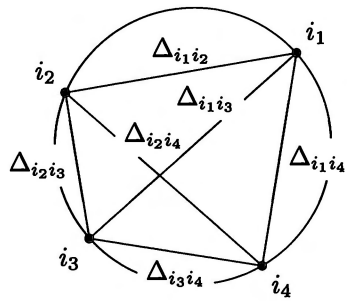


Figure 2.1
Une relation de Ptolémée

classe d'équivalence notée $[v] = [v_1 : \cdots : v_N]$ d'un vecteur non nul $v = (v_1, \ldots, v_N)$ de p, où l'on identifie $(v_1, \ldots, v_N)$ et $(\lambda v_1, \ldots, \lambda v_N)$ pour tout $\lambda \in \mathbb{K}^*$.
On notera parfois, par abus, $v = (v_i) \in \mathbb{P}(\mathbb{K}^N)$, ce qui sera assez pratique, mais manquant cruellement de sens, vu que les v_i dépendent alors d'un représentant de v dans $\mathbb{K}^N$.
Si $F(X_1, \ldots, X_N)$ est un polynôme quelconque en N indéterminées, la valeur $F(x_1, \ldots, x_N)$ dépend bien entendu du choix d'un vecteur directeur $(x_1, \ldots, x_N)$ de p. Mais si F est *homogène*, c'est-à-dire si pour un entier d convenable, on a : $F(\lambda x_1, \ldots, \lambda x_N) = \lambda^d F(x_1, \ldots, x_N)$ pour tous $\lambda \in \mathbb{C}^*$ et $(x_1, \ldots, x_N) \in \mathbb{K}^N$, alors l'équation $F(x_1, \ldots, x_N) = 0$ est une réunion de droites vectorielles (ce qui caractérise un cône de $\mathbb{K}^N$), et définit donc une partie de $\mathbb{P}(\mathbb{K}^N)$. Autrement dit, la validité de l'assertion $F(x_1, \ldots, x_N)$ ne dépend que de p et non pas du vecteur directeur choisi v. On écrira par abus : $F(p) = 0$. Cela précède s'étend à une famille de polynômes homogènes, même si leurs degrés sont différents.

Le résultat central de cette partie est la description du plongement de Plücker par un système d'équations homogènes de l'image de la grassmannienne $\mathrm{Gr}_{r,n}$ dans $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$.

2.9. Théorème. *Soient r et n deux entiers, avec $0 < r < n$. Soit $\psi = \psi_{r,n}$ le plongement de Plücker de la grassmannienne $\mathrm{Gr}_{r,n}$ dans $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$: l'image d'un sous-espace F est le point $[\Lambda^r(A_F)]$, où A_F est une matrice de $\mathscr{M}_{n,r}(\mathbb{K})$ dont les colonnes forment une base du sous-espace F.*

L'image de ψ est l'ensemble des points $v = [(v_K)_{K \in \Lambda(r,n)}]$ de $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$ tels que les relations de Plücker (notées également $\mathscr{P}_{I,J}$)

$$\mathscr{P}_{I,J}(v) = \sum_{k,\ j_k \notin I} (-1)^{k+\iota(I,j_k)} v_{I \cup \{j_k\}} v_{J \setminus \{j_k\}} = 0$$

soient satisfaites pour tout I dans $\Lambda(r-1,n)$ et $J = \{j_1 < j_2 < \cdots < j_{r+1}\}$ dans $\Lambda(r+1,n)$.

2.10. Idée-clé. La preuve de ce théorème risque de sembler un peu longue. Mais les idées sont simples. Nous devons montrer que l'image de ψ est égale à un certain ensemble algébrique. Nous allons procéder par double inclusion. Pour la première inclusion, on constate que la formule algébrique désirée provient de l'annulation du déterminant d'une matrice dont deux colonnes ont été répétées.

Pour ce qui est de l'inclusion inverse, un débriefing sera proposé à la suite dans la remarque 2.11.

Démonstration. On a montré ci-dessus que ψ était bien définie, injective, et qu'elle commutait avec l'action du groupe linéaire. Reste à montrer l'assertion sur la caractérisation de l'image. On doit montrer que l'image de ψ est l'ensemble V des points $[(v_K)_{K\in\Lambda(r,n)}]$ de $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$ tels que

$$\sum_{k,\ j_k\notin I} (-1)^{k+\iota(I,j_k)} v_{I\cup\{j_k\}} v_{J\setminus\{j_k\}} = 0$$

pour tout $I \subset [1, r-1]$ et tout $J = \{j_1 < \cdots < j_{r+1}\} \subset [1, n]$.

Première étape : l'inclusion $\psi(\mathrm{Gr}_{r,n}) \subset V$. Il s'agit de montrer que lorsque $A = (a_{ij})$ est une matrice de $\mathscr{M}_{n,r}(\mathbb{K})$, on a : $\mathscr{P}_{I,J}(A) = 0$ pour tous I et J. Soit L_i la i-ème ligne de A. En plaçant L_{j_k} à la dernière ligne puis, en développant par rapport à cette ligne, il vient :

$$(-1)^{\iota(I,j_k)}\Delta_{I\cup\{j_k\}}(A) = \det\begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_{r-1}} \\ L_{j_k} \end{pmatrix} = \sum_{s=1}^{r} (-1)^{r+s} a_{j_k,s}\delta_s,$$

où $\delta_s = \Delta_{I,[1,r]\setminus\{s\}}$. On obtient donc :

$$\mathscr{P}_{I,J}(A) = \sum_{s=1}^{r} (-1)^r \delta_s \Big(\sum_{k=1}^{r+1} (-1)^{k+s} a_{j_k,s}\Delta_{J\setminus\{j_k\}}(A)\Big).$$

Or, en développant la matrice qui suit selon la colonne s qui a été répétée, il vient :

$$\begin{aligned} 0 &= \det\begin{pmatrix} a_{j_1,1} & \cdots & a_{j_1,s} & a_{j_1,s} & \cdots & a_{j_1,r} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{j_{r+1},1} & \cdots & a_{j_{r+1},s} & a_{j_{r+1},s} & \cdots & a_{j_{r+1},r} \end{pmatrix} \\ &= \sum_{k=1}^{r+1} (-1)^{k+s} a_{j_k,s}\Delta_{J\setminus\{j_k\}}(A). \end{aligned}$$

On en déduit finalement : $\mathscr{P}_{I,J}(A) = 0$.

Deuxième étape : l'inclusion $V \subset \psi(\mathrm{Gr}_{r,n})$. Soit donc $v = [(v_K)_{K\in\Lambda(r,n)}] \in V$. On sait qu'au moins une coordonnée de v est non nulle, disons v_L pour

$L = \{\ell_1 \leqslant \cdots \leqslant \ell_r\}$. Soit $P = P_\sigma$ la matrice de permutation où σ est la permutation qui envoie $(\ell_1, \ldots, \ell_r)$ sur $(1, \ldots, r)$, et qui est croissante sur le complémentaire $\bar{L}$. On voit alors en utilisant l'exercice 1.15 que $P_\sigma \cdot v = [(\varepsilon_{K,\sigma^{-1}(K)} v_{\sigma^{-1}(K)})]$, où $\varepsilon_{K,\sigma^{-1}(K)} = 1$, puisque ce nombre désigne la signature de $\phi_K^{-1} \circ \sigma \circ \phi_{\sigma^{-1}(K)}$ qui vaut l'identité, donc 1. Ainsi, comme v satisfait aux relations de Plücker, $P_\sigma \cdot v$ y satisfait également. Donc, en utilisant le fait que ψ commute avec l'action de $\mathrm{GL}_n(\mathbb{K})$, on peut se ramener au cas où $L = \{1, \ldots, r\}$.

On a maintenant : $v_L \neq 0$. Quitte à remplacer v par v/v_L, on peut supposer par homogénéité que $v_L = 1$. On veut trouver un antécédent à v par ψ. Pour cela, on considère le sous-espace F engendré par les colonnes de la matrice $A = (a_{ij})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant r}$ suivante :

$$A = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & \ldots & 1 \\ a_{r+1,1} & a_{r+1,2} & \ldots & a_{r+1,r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,r}, \end{pmatrix},$$

avec :

$$\forall i \in [r+1, n],\ \forall j \in [1, r], \quad a_{ij} = (-1)^{r-j} v_{L \setminus \{j\} \cup \{i\}}.$$

On va montrer que $\Lambda^r(A) = (v_K)_{K \in \Lambda(r,n)}$. Pour cela, on montre par récurrence sur $|L \cap \bar{K}|$ que

$$\Delta_K(A) = \Lambda^r(A)_K = v_K.$$

Si $|L \cap \bar{K}| = 0$, alors $K = L$ et l'on a : $\Lambda^r(A)_L = 1 = v_L$.
Si $|L \cap \bar{K}| = 1$, alors K est de la forme $\{1 < 2 < \cdots < i-1 < i+1 < \cdots < r < k\}$ et, en développant par rapport à la dernière ligne, on trouve :

$$\Lambda^r(A)_K = \det \begin{pmatrix} 1 & 0 & & \ldots & & & 0 \\ 0 & 1 & & \ldots & & & 0 \\ \vdots & \vdots & & \vdots & & & \\ \vdots & & & 0 & 1 & & 0 \\ \vdots & & & & \ddots & & 0 \\ \vdots & \ldots & \ldots & \ldots & \ldots & 0 & 1 \\ a_{k,1} & a_{k,2} & \ldots & a_{k,i} & \ldots & \ldots & a_{k,r} \end{pmatrix}$$

$$= (-1)^{r+i} a_{k,i} = (-1)^{r+i}(-1)^{r-i} v_K = v_K,$$

On suppose la propriété vraie à l'ordre $s-1$. Soit $K = \{k_1 < k_2 < \cdots < k_r\}$ tel que $|L \cap \bar{K}| = s$. On a :

$$\Delta_K(A) = \det \begin{pmatrix} a_{k_1,1} & \cdots & a_{k_1,r} \\ \vdots & \vdots & \vdots \\ a_{k_r,1} & \cdots & a_{k_r,r} \end{pmatrix} = \sum_{i=1}^{r} (-1)^{r+i} a_{k_r,i} m_{k_r,i},$$

où $m_{k_r,i}$ est le mineur de la matrice A_K à laquelle on a ôté la ligne k_r et la colonne i. Posons

$$I = K \setminus \{k_r\} = \{k_1 < k_2 < \cdots < k_{r-1}\}.$$

Pour $1 \leqslant i \leqslant r$, la i-ème ligne de A est $(0 \cdots 0\ 1\ 0 \cdots 0)$: en développant $\Delta_{I\cup\{i\}}(A)$ par rapport à la ligne i, on trouve :

$$\Delta_{I\cup\{i\}}(A) = (-1)^{r-i}(-1)^{\iota(I,i)} m_{k_r,i}.$$

Par récurrence, puisque $|L \cap \overline{I \cup \{i\}}| = s-1$, on a : $\Delta_{I\cup\{i\}}(A) = v_{I\cup\{i\}}$. Ainsi, en posant $J = \{1, 2, \ldots, r, k_r\}$, il vient :

$$\begin{aligned} \Delta_K(A) &= \sum_{i=1}^{r} (-1)^{r+i} a_{k_r,i} (-1)^{r-i} (-1)^{\iota(I,i)} \Delta_{I\cup\{i\}} \\ &= \sum_{i=1}^{r} (-1)^{r+i} (-1)^{\iota(I,i)} v_{J\setminus\{i\}} v_{I\cup\{i\}}. \end{aligned}$$

Il est maintenant temps d'utiliser les relations de Plücker pour v. Plus précisément, la relation de Plücker $\mathscr{P}_{I,J}$ donne

$$0 = \mathscr{P}_{I,J}(v) = \sum_{i=1}^{r} (-1)^{i} (-1)^{\iota(I,i)} v_{J\setminus\{i\}} v_{I\cup\{i\}} + (-1)^{r+1} v_K v_L.$$

En comparant avec l'expression obtenue pour $\Delta_K(A)$, compte tenu du fait que $v_L = 1$, on a bien : $\Delta_K(A) = v_K$, comme souhaité. □

2.11. Remarques. Géométriquement, la condition $\Delta_L(A) \neq 0$ signifie que l'espace F engendré par les colonnes de A est un *supplémentaire* de l'espace $S_{\bar{L}}$ engendré par les vecteurs e_i, $i \notin L$ de la base canonique. En effet, les classes des $(e_k)_{k\in L}$ forment une base du quotient $\mathbb{K}^n/S_{\bar{L}}$ et passer au quotient, c'est essentiellement « oublier » les lignes de $\bar{L}$. Alors, $\Delta_L(A)$ n'est pas nul si et seulement si l'image d'une base de F engendre le quotient, ce qui revient à dire que F est un supplémentaire.

La matrice A de la preuve précédente semble parachutée. En fait, celle-ci est relativement naturelle. On cherche la matrice A d'une base d'un sous-espace F, sachant que le mineur de A d'indice $L = \{1, \ldots, r\}$ n'est pas

nul. Quitte à multiplier à droite par l'inverse de la sous-matrice formée des r premières lignes de A, on peut supposer que cette sous-matrice est l'identité. (Conceptuellement, cela revient à chercher une base de F qui relève l'image de la base canonique dans le quotient $\mathbb{K}^n/S_{\bar{L}}$, sachant que F est un supplémentaire de $S_{\bar{L}}$.) Mais alors, on constate que les coefficients de A sont des mineurs de A (au signe près ; cette remarque est la partie « $s = 1$ » de la récurrence). On n'a donc guère le choix.

Dans la suite, on s'intéresse au comportement des coordonnées de Plücker vis-à-vis des opérations usuelles de l'algèbre linéaire : somme directe, orthogonal, intersection...

2.12. Coordonnées de Plücker d'une somme directe

Grâce à la formule de Laplace 1.8, on va pouvoir déterminer les coordonnées de Plücker de la somme de deux sous-espaces qui sont en somme directe.

Considérons donc deux sous-espaces F et F' en somme directe dans $\mathbb{K}^n$, de dimensions respectives r et r'. Soient $A_F \in \mathscr{M}_{n,r}$ et $A_{F'} \in \mathscr{M}_{n,r'}$ des matrices génératrices pour F et F'. Alors, en concaténant en colonnes A_F et $A_{F'}$, on obtient une matrice $A_{F\oplus F'} = \begin{pmatrix} A_F & A_{F'} \end{pmatrix} \in \mathscr{M}_{n,r+r'}$. Le développement du déterminant de Laplace donne, pour toute partie $K \in \Lambda(r+r', n)$:

$$\Delta_K(A_{F\oplus F'}) = \sum_{I\subset K,\ |I|=r} (-1)^{\ell(I,K\setminus I)} \Delta_I(A_F)\Delta_{K\setminus I}(A_{F'}).$$

On en déduit le résultat suivant.

2.13. Théorème. *Soient F et F' deux sous-espaces en somme directe de $\mathbb{K}^n$ de dimensions respectives r et r'. Notons $\psi(F) = [v_I]_{I\in\Lambda(r,n)}$ et $\psi(F') = [v'_I]_{I\in\Lambda(r,n)}$. Alors, $\psi(F\oplus F') = [w_K]_{K\in\Lambda(r+r',n)}$ où, pour toute partie $K \in \Lambda(r+r', n)$:*

$$w_K = \sum_{I\subset K,\ |I|=r} (-1)^{\ell(I,K\setminus I)} v_I v'_{K\setminus I}.$$

2.14. Remarque. Notons que si F et F' ne sont pas en somme directe, alors le membre de droite a encore un sens. Il représente alors un mineur de taille $\dim F + \dim F'$ d'une matrice concaténée $\begin{pmatrix} A_F & A_{F'} \end{pmatrix}$, laquelle a pour rang $\dim(F + F')$. Le mineur est donc nul : avec $\psi(F) = [v_I]_{I\in\Lambda(r,n)}$ et $\psi(F) = [v'_I]_{I\in\Lambda(r,n)}$, on a :

$$\forall K \in \Lambda(r+r', n), \quad \sum_{I\subset K, |I|=r} (-1)^{\ell(I,K\setminus I)} v_I v_{K\setminus I} = 0.$$

2.15. Coordonnées de Plücker de l'orthogonal d'un sous-espace

Munissons $\mathbb{K}^n = \mathscr{M}_{n,1}(\mathbb{K})$ de sa forme bilinéaire symétrique canonique : $\langle u, v\rangle = {}^t uv$. On va exprimer simplement les coordonnées de Plücker de l'orthogonal $F^\perp$ d'un sous-espace F en fonction de celles de F. La preuve proposée ici utilise une généralisation de la formule qui relie, pour A carrée de taille n, la matrice $\Lambda^{n-1}(A)$ et la comatrice $\mathrm{com}(A)$.

2.16. Notations. Soient r, n deux entiers avec $0 < r < n$. On fixe un ordre total $\leqslant$ sur $\Lambda(r,n)$ et l'ordre transposé $\leqslant_t$ sur $\Lambda(n-r,n)$ défini par

$$K \leqslant_t L \;\Leftrightarrow\; \bar{K} \leqslant \bar{L};$$

autrement dit, une partie $K \in \Lambda(r,n)$ et son complémentaire $\bar{K} \in \Lambda(n-r,n)$ ont le même rang d'énumération).

On introduit la matrice diagonale (avec δ symbole de Kronecker) :

$$D_{n-r} = (\delta_{I,J} d_I)_{I,J\in\Lambda(n-r,n)}, \quad \text{où } d_I = (-1)^{\ell(I)} \ (I \in \Lambda(n-r,n)).$$

On remarque que l'on a : $D_{n-r} = (-1)^{r(n-r)} D_r$, d'après le lemme 1.7.

On va calculer les coordonnées de Plücker de l'orthogonal. Le produit par D_{n-r} est l'action d'un élément de $\mathrm{GL}(\mathbb{K}^{\Lambda(r,n)})$ sur $\mathbb{P}(\mathbb{K}^{\Lambda(n-r,n)})$.

2.17. Théorème. *Soit F un sous-espace de dimension r de $\mathbb{K}^n$. Alors, on a dans $\mathbb{P}(\mathbb{K}^{\Lambda(r,n)})$:*

$$\psi_{n-r,n}(F^\perp) = D_{n-r}\psi_{r,n}(F).$$

Puisque l'action de D_{n-r} sur l'espace projectif est défini à homothétie près, on n'aurait rien changé à la formule en prenant $d_I = (-1)^{\ell(\bar{I})}$. En effet : $\ell(I) + \ell(\bar{I}) = r(n-r)$, qui est indépendant de I.

Avant de rentrer dans une preuve du théorème, on renormalise les Λ. Soit, pour $A \in \mathscr{M}_{n,r}(\mathbb{K})$:

$$\tilde{\Lambda}^{n-r}(A) = D_{n-r}\Lambda^{n-r}(A) = \big((-1)^{\ell(I)}\Delta_I(A)\big)_{I\in\Lambda(n-r,n)}$$

et, pour $P \in \mathscr{M}_n(\mathbb{K})$:

$$\Lambda_{n-r}(P) = D_{n-r}\Lambda^{n-r}(P)D_{n-r}^{-1} = \big((-1)^{\ell(I)+\ell(J)}\Delta_{I,J}(P)\big)_{I,J\in\Lambda(n-r,n)}.$$

On a donc

$$\tilde{\Lambda}^{n-r}(PA) = D_{n-r}\Lambda^{n-r}(PA) = D_{n-r}\Lambda^{n-r}(P)\Lambda^{n-r}(A),$$

d'où :

$$\tilde{\Lambda}^{n-r}(PA) = \Lambda_{n-r}(P)\tilde{\Lambda}^{n-r}(A).$$

La proposition suivante est une étape clé dans la preuve du théorème.

2.18. Proposition. *Soit P dans $\mathscr{M}_n(\mathbb{K})$. Alors*

$$\Lambda^r(P)\Lambda_{n-r}({}^tP) = \det(P)\mathrm{I}_{\binom{n}{r}}.$$

Démonstration. Soit $\mathscr{D}$ la matrice $\Lambda^r(P)\Lambda_{n-r}({}^tP)$. Nous voulons donc montrer que $\mathscr{D}_{I,I'} = \det(P)\delta_{I,I'}$, avec $I, I' \in \Lambda(r,n)$, où δ est le symbole de Kronecker.

Premier cas : $I = I'$. L'ordre que l'on a mis sur les deux matrices implique, par la formule de Binet-Cauchy, que l'on a :

$$\begin{aligned}\mathscr{D}_{I,I} &= \sum_J \Delta_{I,J}(P)\Delta_{\bar{J},\bar{I}}({}^tP)(-1)^{\ell(\bar{I})+\ell(\bar{J})} \\ &= \sum_J \Delta_{I,J}(P)\Delta_{\bar{I},\bar{J}}(P)(-1)^{\ell(I)+\ell(J)} \\ &= \det(P).\end{aligned}$$

Deuxième cas : $I \neq I'$. On calcule de même :

$$\begin{aligned}\mathscr{D}_{I,I'} &= \sum_J \Delta_{I,J}(P)\Delta_{\bar{I},\bar{J}}(P)(-1)^{\ell(I')+\ell(J)} \\ &= (-1)^{\ell(I')}\sum_J \Delta_{I,J}(P)\Delta_{\bar{I},\bar{J}}(P)(-1)^{\ell(J)}.\end{aligned}$$

On introduit une matrice $\tilde{P}$ de $\mathscr{M}_n(\mathbb{K})$ en décrivant ses lignes $L_i(\tilde{P})$ en fonction des lignes $L_i(P)$ de P :

- si $i \in I$, alors $L_i(\tilde{P}) = L_i(P)$;
- si $i \notin I$, alors $L_i(\tilde{P}) = L_{\sigma(i)}(P)$, où σ est l'unique permutation de $[1,n]$ croissante sur I et croissante sur $\bar{I}$ qui envoie I sur I' et $\bar{I}$ sur $\bar{I}'$.

D'une part, comme I et I' sont distincts et de même cardinal, il vient : $|I \cap \bar{I}'| > 0$. Deux lignes de $\tilde{P}$ sont donc égales, d'où : $\det\tilde{P} = 0$. D'autre part, l'ensemble des lignes $\{L_i(\tilde{P}),\ i \notin I\}$ est exactement l'ensemble des lignes $\{L_i(P),\ i \in \bar{I}'\}$ dans le même ordre. Ainsi, $\Delta_{\bar{I},\bar{J}}(\tilde{P}) = \Delta_{\bar{I}',\bar{J}}(P)$.

Grâce à ce qui précède et au développement de Laplace du déterminant de $\tilde{P}$, on a :

$$\begin{aligned}0 = \det\tilde{P} &= \sum_{J\in\Lambda(r,n)} \Delta_{I,J}(\tilde{P})\Delta_{\bar{I},\bar{J}}(\tilde{P})(-1)^{\ell(J)+\ell(I)} \\ &= (-1)^{\ell(I)-\ell(I')}\sum_{J\in\Lambda(r,n)} \Delta_{I,J}(P)\Delta_{\bar{I}',\bar{J}}(P)(-1)^{\ell(J)+\ell(I')}.\end{aligned}$$

On obtient bien : $\mathscr{D}_{I,I'} = 0$, comme désiré. □

Démonstration (*du théorème*). On commence par un cas particulier. Soit F_0 l'espace engendré par les r premiers vecteurs de la base canonique de $\mathbb{K}^n$; son orthogonal $F_0^\perp$ est engendré par les $n-r$ derniers. On engendre F_0 (resp. B_0) par les colonnes de la matrice A_0 (resp. B_0) formée des r premières (resp. des $n-r$ dernières) colonnes de l'identité I_n. Remarquons que le rang de A_0 est r, celui de B_0 est $n-r$ et que ${}^tB_0A_0 = 0$. On a de plus par un calcul immédiat :

$$\Lambda^{n-r}(B_0) = D_{n-r}\Lambda^r(A_0),$$

(le seul coefficient non nul correspond à l'indice $[1,r]$ ou $[r+1,n]$ et $\ell([1,r])=1$), d'où :

$$D_{n-r}\psi(F_0) = [1,0\ldots,0] = \psi(F_0^\perp).$$

À présent, soit F un sous-espace de dimension r de $\mathbb{K}^n$. Il existe une matrice inversible P qui envoie F_0 sur F. Soit $A = PA_0$: ses colonnes engendrent F. Soit aussi : $B = {}^tP^{-1}B_0$. C'est une matrice de rang $n-r$ et on a : ${}^t({}^tP^{-1}B_0)(PA_0) = {}^tB_0A_0 = 0$. Par suite, les colonnes de B engendrent $F^\perp$.

Il ne reste plus qu'à montrer que $\Lambda^{n-r}(B)$ et $D_{n-r}\Lambda^r(A)$ sont égales à scalaire près. On utilise la multiplicativité des Λ et la proposition 2.18 (appliquée à ${}^tP$) :

$$\begin{aligned}\Lambda^{n-r}(B) &= \Lambda^{n-r}({}^tP^{-1}B_0) = \Lambda^{n-r}({}^tP)^{-1}\Lambda^{n-r}(B_0)\\ &= \frac{1}{\det P}\Lambda_r(P)D_{n-r}\Lambda^r(A_0) = \frac{1}{\det P}D_{n-r}\Lambda^r(P)\Lambda^r(A_0)\\ &= \frac{1}{\det P}D_{n-r}\Lambda^r(A).\end{aligned}$$

Cela achève la preuve du théorème. □

2.19. Exemple. Soit $n=3$, $r=1$, alors l'ordre naturel sur $\Lambda(1,3) = \{1 < 2 < 3\}$ implique l'ordre $\{2,3\} < \{1,3\} < \{1,2\}$ sur $\Lambda(2,3)$. La matrice D_2 est donc la matrice diagonale $\mathrm{diag}(1,-1,1)$. Soit F la droite engendrée par le vecteur colonne ${}^t(a,b,c)$. D'après le théorème, on a $\psi_{2,3}(F^\perp) = D_2\psi_{1,3}(F) = (a:-b:c)$.

Cela peut être facilement vérifié, car $F^\perp$ est engendré par ${}^t(0,-c,b)$ et ${}^t(-b,a,0)$.

2.20. Remarque. Au fond, le théorème précédent ne parle pas vraiment d'orthogonal pour la forme $\langle\cdot,\cdot\rangle$, mais plutôt de dualité. Il faut alors interpréter B comme la matrice d'un système d'équations de F, ce qui justifie que l'action de la matrice de passage P sur B fasse intervenir la transposée de l'inverse.

2.21. Corollaire. *Soit $A \in \mathscr{M}_{n,r}(\mathbb{K})$ $\big($resp. $B \in \mathscr{M}_{n,n-r}(\mathbb{K})\big)$, une matrice de rang r (resp. $n-r$). Si ${}^tBA = 0$, alors $\Lambda^{n-r}(B)$ et $D_{n-r}\Lambda^r(A)$ sont égales à un scalaire non nul près.*

2.22. Coordonnées de Plücker d'une intersection

On termine avec le séduisant théorème qui donne les coordonnées de Plücker de l'intersection de deux sous-espaces en fonction des coordonnées de Plücker de ces sous-espaces. Sa preuve réside essentiellement en une synthèse des deux résultats précédents sur les coordonnées de Plücker de la somme directe et de l'orthogonal en remarquant que $F \cap F' = (F^\perp + F'^\perp)^\perp$.

2.23. Théorème. *Soient F et F' deux sous-espaces de K^n de dimensions respectives r et r' et tels que $F+F' = \mathbb{K}^n$. Alors, les coordonnées de Plücker de $F \cap F'$ sont, à scalaire près indépendant de I dans $\Lambda(r+r'-n,n)$:*

$$\psi(F \cap F')_I = \sum_{J,J'} (-1)^{\iota(J,J')} \psi(F)_{I\cup J} \psi(F')_{I\cup J'},$$

où la somme porte sur tous les $J \in \Lambda(n-r',n)$, $J' \in \Lambda(n-r,n)$ tels que $\{I,J,J'\}$ soit une partition de $[1,n]$.

Démonstration. L'hypothèse $F+F' = \mathbb{K}^n$ implique que $F^\perp \cap F'^\perp = (F+F')^\perp = \{0\}$ et donc par le théorème 2.13

$$\psi(F^\perp \oplus F'^\perp)_L = \sum_{J\subset L,\ |J|=n-r} (-1)^{\iota(J,L\setminus J)} \psi(F^\perp)_J \psi(F'^\perp)_{L\setminus J}.$$

En utilisant le théorème 2.17, on déduit, pour tout I dans $\Lambda(r+r'-n,n)$:

$$\begin{aligned}
\psi(F\cap F')_I &= \psi\big((F^\perp \oplus F'^\perp)^\perp\big)_I = (-1)^{\ell(I)} \psi(F^\perp \oplus F'^\perp)_{\bar I} \\
&= (-1)^{\ell(I)} \sum_{K\subset \bar I,\ |K|=n-r} (-1)^{\iota(K,\bar I\setminus K)} \psi(F^\perp)_K \psi(F'^\perp)_{\bar I\setminus K} \\
&= (-1)^{\ell(I)} \sum_{K\subset \bar I, |K|=n-r} (-1)^{\iota(K,\bar I\setminus K)} (-1)^{\ell(K)} \psi(F)_{\bar K} (-1)^{\ell(\bar I\setminus K)} \psi(F')_{\overline{\bar I\setminus K}} \\
&= (-1)^{\ell(I)} \sum_{K\subset \bar I, |K|=n-r} (-1)^{\iota(K,\bar I\setminus K)} (-1)^{\ell(K)} \psi(F)_{\bar K} (-1)^{\ell(\bar I\setminus K)} \psi(F')_{I\cup \bar K}.
\end{aligned}$$

Posons $J = \bar I \setminus K$ et $J' = K$ de sorte que (puisque $K \subset \bar I$), $\bar K = I \cup J$, $I \cup \bar K = I \cup J'$ et $I \cup J \cup J' = [1,n]$, toutes les réunions étant disjointes.

On obtient donc $\psi(F\cap F')_I = \sum_{J,J'} \varepsilon_{J,J'} \psi_{I\cup J}(F) \psi_{I\cup J'}(F')$, avec $\varepsilon(J,J') = (-1)^{\ell(I)+\iota(J',J)+\ell(J')+\ell(J)}$. Or, $\iota(J,J') + \iota(J',J)$ ne dépend pas de (J,J') par 1.7. De plus, $\ell(J') + \ell(J) = \ell(J') + \ell(\bar I \setminus J') = \ell(\bar I) = n(n-r) - \ell(I)$. Cela fournit le résultat annoncé. □

2.24. Remarque. Si les sous-espaces F et F' ne vérifient pas l'hypothèse $F + F' = \mathbb{K}^n$, alors on montre en suivant la preuve que

$$\sum_{J,J'} (-1)^{\iota(J,J')} \psi(F)_{I\cup J} \psi(F')_{I\cup J'} = 0$$

pour tout I.

2.25. Remarque. Ce théorème fait entrevoir la possibilité de comprendre des intersections en travaillant dans une algèbre. On trouvera, dans les exercices du paragraphe C, une façon élémentaire d'aborder le problème dans un cadre simple (intersection de sous-espaces d'un espace donné). Nous présentons tout d'abord l'algèbre extérieure avec les moyens du bord, puis nous tordons le produit extérieur pour obtenir un produit d'intersection. Le lecteur intéressé par cette approche peut s'initier avec le livre *Young Tableaux* [29] de William Fulton avant d'attaquer le coriace *Intersection Theory* [30] du même auteur.

Vous, vous, vous, c'était bien, là-bas.
Vous, c'était bien... enfin c'était... comme ci comme ça.

3. Décomposition de Bruhat

3.1. Type d'un sous-espace par rapport au drapeau standard

On reprend les notations du chapitre IV du tome premier. On note G le groupe linéaire $\mathrm{GL}_n(\mathbb{K})$, B le sous-groupe de G formé des matrices triangulaires supérieures.

Un *drapeau complet* de $\mathbb{K}^n$ est une suite $(F_0, \dots, F_n)$ de sous-espaces tels que $\dim(F_k) = k$ et $F_k \subset F_{k+1}$ pour tout k. Le *drapeau standard* est le drapeau $F_\bullet^{\mathrm{std}} = (F_k^{\mathrm{std}})_{0\leqslant k\leqslant n}$ où, pour tout k, F_k^{std} est engendré par les k premiers vecteurs de la base standard $\mathbf{e} = (e_1, \dots, e_n)$ de $\mathbb{K}^n$.

Soit k un entier compris entre 1 et n. L'ensemble $\mathrm{Gr}_{k,n}$ des sous-espaces de dimension k est appelé la *grassmannienne* des k-plans de $\mathbb{K}^n$. L'action naturelle de G est transitive : tous les k-plans sont dans l'orbite de F_k^{std} ; le stabilisateur de F_k^{std} est le groupe P_k des matrices

$$\begin{pmatrix} g_1 & g_2 \\ 0 & g_3 \end{pmatrix}, \quad \text{où } g_1 \in \mathrm{GL}_k(\mathbb{K}),\ g_3 \in \mathrm{GL}_{n-k}(\mathbb{K}),\ g_2 \in \mathscr{M}_{k,n-k}(\mathbb{K}).$$

Ainsi, l'application $G \to \mathrm{Gr}_{k,n}$, $g \mapsto gF_\bullet^{\mathrm{std}}$ induit une bijection (homéomorphisme si cela a un sens) $\varphi_k : G/P_k \to \mathrm{Gr}_{k,n}$, décrite ainsi : $\varphi_k(gP_k)$ est l'espace engendré par les k premières colonnes de g (il ne dépend que de gP_k).

Reste une action naturelle de B à gauche sur la grassmannienne (via l'identification, l'action de $b \in B$ sur $gP_k \in G/P_k$ est simplement : $b{\cdot}gP_k = bgP_k$).

Étant donné un k-plan F de $\mathbb{K}^n$, la suite $\dim(F \cap F_j^{\mathrm{std}})$ est croissante et les quotients successifs $(F \cap F_j^{\mathrm{std}})/(F \cap F_{j-1}^{\mathrm{std}})$ s'injectent dans les droites $F_j^{\mathrm{std}}/F_{j-1}^{\mathrm{std}}$, ce qui implique la dimension de $(F \cap F_j^{\mathrm{std}})/(F \cap F_{j-1}^{\mathrm{std}})$ vaut 0 ou 1. On repère les sauts de dimension : soit $\mathbf{i}$ l'ensemble des indices i tels que $\dim(F \cap F_i^{\mathrm{std}})/(F \cap F_{i-1}^{\mathrm{std}}) = 1$: c'est une partie à k éléments $\mathbf{i} = \{i_1 < \cdots < i_k\}$. On l'appelle le *type* de F. D'après [H2G2, théorème IV-3.2.4], le type de F permet de caractériser la B-orbite de F, de la décrire et de lire son adhérence. Plus précisément...

3.2. Proposition. *Soient F et F' deux k-plans de $\mathbb{K}^n$ et $\mathbf{i}=\{i_1<\cdots<i_k\}$ et $\mathbf{i}' = \{i'_1 < \cdots < i'_k\}$ leurs types respectifs. Alors :*

(i) *les k-plans F et F' sont dans la même B-orbite si et seulement si $\mathbf{i} = \mathbf{i}'$;*

(ii) *la B-orbite de F est en bijection avec $\mathbb{K}^d$, où $d = \sum_{j=1}^{k}(i_j - 1)$;*

(iii) *($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) le k-plan F appartient à l'adhérence de la B-orbite de F' si et seulement si $i_1 \leqslant i'_1, \ldots, i_k \leqslant i'_k$.*

3.3. Exemple. Pour tout (a, b) dans $\mathbb{K}^2 \setminus \{(-1, 1)\}$, décrivons le plan $F = F_{a,b}$ suivant de $\mathbb{K}^3$ par la matrice A_F d'une base dans la base canonique :

$$\begin{pmatrix} 1 & -1 \\ a & 1 \\ a & b \end{pmatrix}.$$

Alors, F est de type $\{1, 2\}$, pour $a = b = 0$, $\{1, 3\}$, pour $a = 0$, $b \neq 0$, et $\{2, 3\}$ si $a \neq 0$. Si a et b ne sont pas nuls, on voit, en faisant tendre b, puis a vers 0, que $F_{0,0}$ est dans l'adhérence de la B-orbite de $F_{0,b}$, lui-même, dans l'adhérence de la B-orbite de $F_{a,b}$.

3.4. Remarque. Pour $n = 3$, l'ordre de dégénérescence des B-orbites est total, comme on vient de le voir, dans le cadre des plans, dans l'exemple qui précède. En revanche, pour $n \geqslant 4$, l'ordre n'est plus total : on ne peut pas comparer, pour la dégénérescence, un plan de type $\{2, 3\}$ et un plan de type $\{1, 4\}$.

3.5. Orbites de B dans l'espace des drapeaux

On passe à présent des sous-espaces aux drapeaux.

D'après le théorème de la base incomplète, l'action de G sur les drapeaux est transitive. L'application orbitale $g \mapsto \big(\varphi_j(g)\big)_{1 \leqslant j \leqslant k}$ est surjective ; le stabilisateur du drapeau standard $V_\bullet$ est B. Par suite, l'ensemble des *drapeaux complets* $\mathscr{B}$, appelé *variété des drapeaux*[7], s'identifie à G/B.

[7]Dans cet ouvrage, on ne met pas de structure de variété sur l'ensemble ou l'espace topologique $\mathscr{B}$. Pour cela, voir par exemple [63, exercice E.132].

Fixons k entre 1 et n. Remarquons une fois pour toutes que $\mathscr{B}$ est naturellement une partie du produit des grassmanniennes $\prod_{j=0}^{n} \mathrm{Gr}_{j,n}$, que P_k contient B et que l'on a un diagramme commutatif dont les flèches horizontales sont bijectives :

$$\begin{array}{ccc} G/B & \xrightarrow{(\varphi_j)_{0\leqslant j\leqslant n}} & \mathscr{B} \subset \prod_{j=0}^{n} \mathrm{Gr}_{j,n} \\ \downarrow & & \downarrow p_k \\ G/P_k & \xrightarrow{\varphi_k} & \mathrm{Gr}_{k,n}, \end{array}$$

où p_k est la k-ième projection naturelle de $\prod_{j=0}^{n} \mathrm{Gr}_{j,n}$ sur $\mathrm{Gr}_{k,n}$.

On veut classer les B-orbites dans $\mathscr{B}$. Cela revient à étudier les B-orbites dans son action à gauche sur $\mathrm{GL}_n(\mathbb{K})/B$, ce qui donne lieu au quotient noté $B\backslash \mathrm{GL}_n(\mathbb{K})/B$.

Il est presque équivalent d'étudier les orbites de l'action de $B \times B$ sur G donnée par $(b, b') \cdot g = bgb'^{-1}$. Ensemblistement, il y a une bijection entre les double-classes, c'est-à-dire les $B \times B$-orbites dans G et les B-orbites de G/B ; topologiquement, la projection naturelle $G \to G/B$ est ouverte et continue ; elle échange donc les propriétés des $B \times B$-orbites dans G et B-orbites dans G/B.

En traduisant l'action de $B \times B$ en opérations sur les rangées, on est ainsi ramené au problème d'algèbre linéaire élémentaire suivant : étant donnée une matrice $n \times n$ inversible, trouver une forme normale pour les opérations suivantes :

- produit d'une ligne ou d'une colonne par une constante non nulle,
- combinaison linéaire de la forme $\ell_i \to \ell_i + \alpha \ell_j$, où $\alpha \in \mathbb{K}$ et $i < j$, c'est-à-dire que l'on remplace une ligne par une combinaison linéaire utilisant une ligne située *en-dessous*.
- combinaison linéaire de la forme $c_j \to c_j + \alpha c_i$, où $\alpha \in \mathbb{K}$ et $i < j$, c'est-à-dire que l'on remplace une colonne par une combinaison linéaire utilisant une colonne située *à gauche*.

Autrement dit, on cherche une forme normale pour les matrices inversibles à multiplication à gauche et à droite par des matrices inversibles triangulaires supérieures près.

3.6. Remarque. L'idée de type d'un k-plan suggère d'étudier la position relative d'un drapeau $F_\bullet = (F_k)$ et du drapeau standard $F_\bullet^{\mathrm{std}}$, c'est-à-dire la matrice $\left(\dim(F_i \cap F_j^{\mathrm{std}})\right)_{1\leqslant i,j\leqslant n}$. C'est le contenu de la décomposition de Bruhat.

3.7. Décomposition de Bruhat ensembliste

La preuve des résultats de ce paragraphe est adaptée de [31] et [51]. En jouant sur deux tableaux à la fois, les opérations sur les rangées et la géométrie des drapeaux, on réduit autant que l'on peut la manipulation d'indices.

On commence par résoudre le problème d'algèbre linéaire ci-dessus, à savoir trouver une forme normale d'une matrice inversible à multiplication à droite par une matrice triangulaire près, puis on l'exploite en termes de décompositions du groupe linéaire et de l'espace des drapeaux en cellules/B-orbites.

3.8. Remarque. Le rôle que jouaient les suites $1 \leqslant i_1 < \cdots < i_m \leqslant n$ pour l'étude des grassmanniennes est ici tenu par les permutations. Le groupe symétrique $\mathfrak{S}_n$ est isomorphe au groupe W : si σ est une permutation, on notera w_σ ou, par abus de notation, σ la matrice dont les coefficients d'indices $(\sigma(j), j)$ $(1 \leqslant j \leqslant n)$ valent 1 et les autres coefficients sont nuls.

Comme précédemment, le pivot d'une colonne est le coefficient non nul d'indice maximal (placé le plus bas possible).

3.9. Lemme. *Soit n un entier et soit g une matrice $n \times n$ inversible.*

(i) *Il existe une unique (matrice de) permutation $\sigma \in \mathfrak{S}_n$ et un élément g' de gB tels que :*

  (a) *pour j compris entre 1 et n, le pivot de la colonne j est sur la ligne d'indice $\sigma(j)$;*

  (b) *les pivots de g' valent 1 ;*

(ii) *Il existe une unique matrice g'' dans gB satisfaisant, de plus, à la condition :*

  (c) *les coefficients situés dans la même ligne et à droite d'un pivot sont nuls.*

(iii) *Pour σ fixé, soit $\mathscr{E}_\sigma^\wedge$ l'ensemble des classes gB de matrices satisfaisant aux conditions* (a), (b) *et* (c) *ci-dessus. Alors, $\mathscr{E}_\sigma^\wedge$ est un espace affine de dimension égale au nombre d'inversions*[8] *$N(\sigma)$ de σ.*

Démonstration. (i) *Première étape de la réduction* (existence de σ). Soit g une matrice inversible. En appliquant, sur chaque colonne de g, des opérations élémentaires qui ne font intervenir que les colonnes d'indice plus petit (« plus à gauche »), on transforme g en une matrice g' où le nombre total de zéros apparaissant sur le bas des colonnes est maximal. Appelons ici « pivot » d'une colonne un coefficient non nul situé au-dessus d'une suite de zéros partant du bas de la colonne. Alors, quitte à utiliser des dilatations,

[8] Le nombre d'inversions $N(\sigma)$ d'une permutation σ est défini dans l'annexe A.5.

on peut supposer que les pivots de g' valent 1. Ainsi, on a : $gb = g'$ pour b élément convenable de B et une matrice g' de la forme :

$$g' = \begin{pmatrix} * & * & * & * & 1 & * \\ * & * & 1 & * & 0 & * \\ 1 & * & 0 & * & 0 & * \\ 0 & * & 0 & 1 & 0 & * \\ 0 & 1 & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Le point-clé, c'est que toutes les colonnes de g' ont un nombre de zéros différent : en effet, si deux colonnes c_i et c_j de g' se terminaient par le même nombre de zéros, avec $i < j$, une combinaison linéaire de la forme $c_j \to c_j + \lambda c_i$ ferait apparaître un zéro de plus dans c_j, ce qui contredirait la maximalité dans la définition de g'. De plus, le nombre de zéros varie entre 0 et $n-1$ (g' est inversible) et il y a n colonnes. Donc, l'application qui à une colonne associe le nombre de zéros finaux est une bijection.

Autrement dit, l'application σ, qui à j associe l'indice d'un coefficient non nul de la colonne j de g', est une permutation. C'est-à-dire que la matrice g' satisfait aux conditions (a) et (b).

Deuxième étape (unicité de σ). Montrons que σ est déterminé par le drapeau associé à g. Soit k compris entre 1 et n. On note F_k (resp. F'_k) l'espace engendré par les k premières colonnes de g (resp. σ) : c'est l'image de g (resp. σ) dans la grassmannienne $\mathrm{Gr}_{k,n} \simeq \mathrm{GL}_n(\mathbb{K})/P_k$. Comme les cellules dans la grassmannienne $\mathrm{Gr}_{k,n}$ sont les B-orbites et B est inclus dans P_k, les sous-espaces F_k et F'_k appartiennent à la même cellule ! En particulier, le type de F'_k, au sens de la proposition 3.19, est déterminé par g.

Or, le type de F'_k est donné par les k premières colonnes de g', qui, à permutation des colonnes près, est échelonnée. Le type de F'_k est donc l'unique suite croissante $(i_1, \ldots, i_k)$ telle que $\{i_1, \ldots, i_k\} = \{\sigma(1), \ldots, \sigma(k)\}$.

Comme cela est valable pour tout k, g détermine le « drapeau discret »

$$\{\sigma(1)\} \subset \{\sigma(1), \sigma(2)\} \subset \cdots \subset \{\sigma(1), \ldots, \sigma(n)\},$$

qui détermine σ car on a : $\{\sigma(k)\} = \{\sigma(1), \ldots, \sigma(k)\} \setminus \{\sigma(1), \ldots, \sigma(k-1)\}$ pour tout k. Cela prouve la première assertion du lemme.

(ii) Grâce aux opérations permises sur les colonnes, autrement dit par la multiplication à droite d'un élément de B, on transforme g' en annulant tous les coefficients situés sur la même ligne et à droite d'un pivot ; on construit ainsi une matrice g'' toujours dans gB, satisfaisant encore à (a)

et (b) et, de plus, à (c). Dans l'exemple ci-dessus, g'' est de la forme :

$$g'' = \begin{pmatrix} * & * & * & * & 1 & 0 \\ * & * & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & * & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Pour prouver que g'' est unique, il suffit de prouver que si g' et g'' satisfont aux trois conditions, si $g'' = g'b$ pour b dans B, alors $g' = g''$. Pour cela, fixons un indice de colonne j entre 1 et n. Observons les lignes $\sigma(1),\ldots,$ $\sigma(j)$ de g' et g''. Les pivots de ces lignes sont sur les colonnes $1,\ldots, j$, c'est-à-dire, à part le dernier, à gauche de la colonne j. Si l'on écrit ces lignes dans l'ordre ci-dessus, on obtient :

$$\begin{array}{lcccccc} \text{ligne } \sigma(1): & (1 & 0 & \cdots & 0 & 0 & \cdots) \\ \text{ligne } \sigma(2): & (* & 1 & & \vdots & 0 & \cdots) \\ & \vdots & \ddots & \ddots & 0 & \vdots & \\ \text{ligne } \sigma(j): & (* & \cdots & * & 1 & 0 & \cdots). \end{array}$$

Par conséquent, on a :

$$g'_{\sigma(1),j} = 0 = g''_{\sigma(1),j}, \cdots,\ g'_{\sigma(j-1),j} = 0 = g''_{\sigma(j-1),j},\ g'_{\sigma(j),j} = 1 = g''_{\sigma(j),j}.$$

En multipliant g' par la matrice triangulaire b, on obtient g''. Les lignes d'indice $\sigma(1),\ldots,\sigma(j)$ de la matrice $g'b = g''$ constituent un système linéaire en $(b_{1j},\ldots,b_{jj})$ dont, à permutation des équations près, la matrice est l'identité (matrice extraite de g') et le second membre est ${}^t(0\ \cdots\ 0\ 1)$ (partie de la j-ème colonne de g''). Il vient, de proche en proche :

$$b_{1,j} = b_{2,j} = \cdots = b_{j-1,j} = 0, \quad b_{j,j} = 1.$$

On en déduit que b est l'identité et que g' et g'' sont égales, comme annoncé.

(iii) Par définition, $\mathscr{C}_\sigma^\wedge$ est un sous-espace affine de l'espace des matrices. Sa dimension est le nombre de coefficients marqués d'une « $*$ ». Dans l'exemple de g'' ci-dessus, la permutation associée est $\sigma = (1325)$: ses inversions sont $\{(1,3),(1,5),(2,3),(2,4),(2,5),(3,5),(4,5)\}$, en nombre égal aux étoiles de la matrice g''.

Revenons au cas général. Dans la colonne j, les coefficients apparaissant à la ligne du pivot ou en-dessous, *i.e.* d'indice supérieur ou égal à $\sigma(j)$, sont déterminés ; les coefficients libres, c'est-à-dire qui ne sont pas affectés par les conditions (a), (b) et (c), sont ceux qui apparaissent à une ligne $i < \sigma(j)$ tels que le pivot situé à la ligne i est à droite de la colonne j, c'est-à-dire

tels que $j < \sigma^{-1}(i)$. Le nombre de coefficients libres est donc :

$$\big|\{(i,j),\ i < \sigma(j) \text{ et } j < \sigma(i)\}\big| = \big|\{(k,j),\ \sigma(k) < \sigma(j) \text{ et } j < k\}\big| = N(\sigma),$$

qui est, par définition, le nombre d'inversions de σ. □

3.10. Exemple. Si $g = \left(\begin{smallmatrix} 1 & -1 & 1 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{smallmatrix}\right)$, on trouve la matrice g'' de forme normale après manipulation des colonnes, successivement, $C_2 \rightsquigarrow C_2 - C_1$, $C_3 \rightsquigarrow C_3 - C_1$, $C_3 \rightsquigarrow C_3 - 2C_2$, puis normalisation $C_2 \rightsquigarrow -C_2$, $C_3 \rightsquigarrow \frac{1}{4}C_3$,

$$g'' = g \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \frac{1}{4} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

La matrice g'' est bien de la forme voulue, dans gB. La permutation associée à g est donc la transposition (13), dont le nombre d'inversions est 3.

La matrice g est donc une matrice de $\mathscr{E}^{\wedge}_{(13)}$. À chaque orbite hB de $\mathscr{E}^{\wedge}_{(13)}$, on associe l'unique matrice de forme normale $h'' = \left(\begin{smallmatrix} a & b & 1 \\ c & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)$. On voit alors que l'application (bijective) qui, à hB, associe (a,b,c) fournit par transport, une structure d'espace affine sur $\mathscr{E}^{\wedge}_{(13)}$, de dimension $N\big((13)\big) = 3$.

On rappelle que la *matrice de permutation* associée à la permutation σ est la matrice $(\delta_{\sigma(i)i})$, ou, si l'on préfère, la matrice qui envoie l'élément e_i de la base canonique sur $e_{\sigma(i)}$. Comme on définit ainsi un morphisme injectif entre les groupes $\mathfrak{S}_n$ et $\mathrm{GL}_n(\mathbb{K})$, il n'y a pas de réel danger à noter encore σ cette matrice.

La décomposition de Bruhat n'est guère qu'une reformulation de l'assertion (i) du lemme.

3.11. Théorème (Décomposition de Bruhat dans le groupe linéaire). *Soit n un entier naturel, soit B le sous-groupe du groupe linéaire formé des matrices triangulaires supérieures et soit W le groupe des matrices de permutations. On a :*

$$\mathrm{GL}_n(\mathbb{K}) = BWB = \bigcup_{\sigma \in W} B\sigma B,$$

où la réunion est disjointe.

Démonstration. Soit g un élément de $\mathrm{GL}_n(\mathbb{K})$. D'après le lemme, il existe b dans B et σ une matrice de permutation tels que $g' = gb^{-1}$ satisfait aux conditions (a) et (b) du lemme. Mais ces conditions signifient qu'après une permutation convenable des colonnes de g' près, g' devient triangulaire supérieure. Plus précisément, $b' = g'\sigma^{-1} = gb^{-1}\sigma^{-1}$ est triangulaire supérieure. On en déduit : $g = b'\sigma b$, d'où le recouvrement de $\mathrm{GL}_n(\mathbb{K})$ par les

double-classes $B\sigma B$. Le fait que les double-classes soient disjointes provient, de façon analogue, de l'unicité de σ dans le lemme. □

3.12. Exemple. Pour reprendre la matrice g de l'exemple 3.10. On trouve

$$g = g'' \begin{pmatrix} 1 & 1 & \frac{1}{4} \\ 0 & -1 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{4} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & \frac{1}{4} \\ 0 & -1 & -\frac{1}{2} \\ 0 & 0 & \frac{1}{4} \end{pmatrix}.$$

De même, si $g_a = \left(\begin{smallmatrix} 1 & -1 & 1 \\ 2 & 1 & 0 \\ a & 1 & 1 \end{smallmatrix}\right)$, pour $a \neq 5$ (pour assurer que $g_a \in \mathrm{GL}_3(\mathbb{K})$), alors, la matrice g_a est dans $B\sigma_a B$, où

$$\sigma_a = \begin{cases} (123) & \text{si } a = 0, \\ (132) & \text{si } a = 2, \\ (13) & \text{sinon.} \end{cases}$$

Un peu comme pour passer des matrices échelonnées aux grassmanniennes, on exploite et on précise le théorème en passant au quotient par B. Soit $\mathscr{B}$ l'espace des *drapeaux complets* de $\mathbb{K}^n$. Il admet une action (continue lorsque cela a un sens) transitive de $\mathrm{GL}_n(\mathbb{K})$, pour laquelle B est le stabilisateur du drapeau complet standard $F_\bullet^{\mathrm{std}} = (F_i^{\mathrm{std}})_{0 \leqslant i \leqslant n}$, (voir par exemple [H2G2, exercice II-F.21]). L'application orbitale en $F_\bullet^{\mathrm{std}}$ induit une bijection (un homéomorphisme si ça a un sens) $G/B \to \mathscr{B}$, $gB \mapsto g \cdot F_\bullet^{\mathrm{std}}$. La transitivité de l'action et la décomposition de Bruhat donnent :

$$\mathscr{B} = \mathrm{GL}_n(\mathbb{K}) \cdot F_\bullet^{\mathrm{std}} = BWB \cdot F_\bullet^{\mathrm{std}} = \bigcup_{\sigma \in W} B\sigma \cdot F_\bullet^{\mathrm{std}}.$$

3.13. Définition. Avec les notations ci-dessus, on appelle *cellules de Schubert* les parties :

$$\mathscr{C}_\sigma = B\sigma \cdot F_\bullet^{\mathrm{std}} \subset \mathscr{B} \qquad (\sigma \in W).$$

Par acquit de conscience, vérifions qu'elles sont disjointes. Pour $W_\bullet = (W_i)_{0 \leqslant i \leqslant n}$ un drapeau complet quelconque, on choisit g un élément de $\mathrm{GL}_n(\mathbb{K})$ tel que $g \cdot F_\bullet^{\mathrm{std}} = W_\bullet$: la classe gB est bien déterminée ; *a fortiori* la double-classe BgB aussi donc la permutation σ telle que g appartient à $B\sigma B$ aussi.

Dans ces conditions, on dit que $W_\bullet$ *est de type* σ (par rapport au drapeau standard).

3.14. Théorème (Décomposition en cellules de la variété des drapeaux). *Soit n un entier et soit $\mathscr{B}$ la variété des drapeaux complets de $\mathbb{K}^n$. Pour σ appartenant au groupe symétrique $\mathfrak{S}_n$, on note $\mathscr{C}_\sigma$ l'ensemble des drapeaux de type σ par rapport au drapeau standard. On a une partition :*

$$\mathscr{B} = \bigcup_{\sigma \in W} \mathscr{B}_\sigma.$$

De plus, pour tout σ de W, il existe une bijection (un homéomorphisme si cela a un sens) $\mathbb{K}^{N(\sigma)} \to \mathscr{C}_\sigma$, où $N(\sigma)$ est le nombre d'inversions de σ.

Démonstration. D'après l'assertion (ii) du lemme, l'application

$$\mathscr{E}_\sigma^\wedge \longrightarrow \mathscr{C}_\sigma, \quad g'' \mapsto g'' \cdot F_\bullet^{\mathrm{std}}$$

est bijective. Comme c'est la restriction d'une application continue ouverte à un espace affine de $\mathrm{GL}_n(\mathbb{K})$ de dimension $N(\sigma)$, le théorème en résulte.□

3.15. Remarque. Cette décomposition se généralise à un groupe classique G (et même au-delà). Il faut alors remplacer B par un sous-groupe résoluble maximal et W par N/T, où T est un sous-groupe fermé connexe nilpotent de B égal à son centralisateur et N est son normalisateur. On montre, comme pour les quotients G/P par des sous-groupes paraboliques ([H2G2, §II-4.3]), que le quotient G/B est [sur le corps $\mathbb{R}$ ou $\mathbb{C}$] un espace topologique compact. Mais l'importance de B vient du fait que G/B est le plus gros quotient compact de G. La décomposition de Bruhat est le point de départ pour étudier la géométrie de $\mathscr{B} = G/B$. L'action de G sur G/B permet, par exemple, de définir les représentations de dimension finie de G. L'apport de Bruhat dépassait donc une interprétation de l'algorithme de Gauss...

3.16. Adhérence des B-orbites et ordre de Bruhat

On s'intéresse ici à l'adhérence des B-orbites pour l'action à gauche de B sur la variété des drapeaux G/B. Il va de soi que le corps $\mathbb{K}$ est ici le corps des réels ou celui des complexes.

Soit $\Lambda(m,n)$ l'ensemble des parties à m éléments de $[1,n]$.

3.17. Définition. On définit un ordre $\preceq_m$ sur $\Lambda(m,n)$ comme suit :

$$I \preceq_m J \text{ si } i_k \leqslant j_k,\ \forall k \in [1,m], \text{ où } I = \{i_1 < \cdots < i_m\},\ J = \{j_1 < \cdots < j_m\}.$$

Il s'agit d'un ordre partiel dont le plus petit élément est $I_m = \{1 < \cdots < m\}$ et le plus grand $\{n-m+1 < \cdots < n\}$. On définit un pré-ordre noté également $\preceq_m$ sur $\mathfrak{S}_n$ par $\sigma' \preceq_m \sigma$ si $\sigma'(I_m) \preceq_m \sigma(I_m)$. On définit enfin un ordre (on vérifie !) appelé *ordre de Bruhat* sur $\mathfrak{S}_n$ par $\sigma' \preceq \sigma$

si $\sigma' \preceq_m \sigma$ pour tout $1 \leqslant m < n$. Le plus petit élément pour l'ordre de Bruhat est l'élément neutre e et le plus grand est la permutation w_0 telle que $w_0(k) = n+1-k$ pour tout k.

3.18. Exercice. *Soit $\mathfrak{P}_m$ le sous-groupe de $\mathfrak{S}_n$ des permutations qui préservent les parties $\{1,\dots,m\}$ et $\{m+1,\dots,n\}$ de $\{1,\dots,n\}$, c'est-à-dire le sous-groupe engendré par les transpositions simples $(i,i+1)$ $(i \neq m)$, d'après le lemme A.1. Montrer que $\preceq_m$ induit un ordre sur $\mathfrak{S}_n/\mathfrak{P}_m$.*

On montrera que $\mathfrak{S}_n/\mathfrak{P}_m \to \Lambda(m,n)$, $\sigma\mathfrak{P}_m \mapsto \sigma(I_m)$ est une bijection.

3.19. Proposition. *Soit n un entier. Soit B le groupe des matrices triangulaires supérieures $n \times n$. Pour σ et σ' deux (matrices de) permutations, il est équivalent de dire :*

(i) $\mathscr{C}_{\sigma'} \subset \overline{\mathscr{C}_\sigma}$;

(ii) *pour m compris entre 1 et n, $\sigma'(I_m) \preceq_m \sigma(I_m)$;*

(iii) $\sigma' \preceq \sigma$.

E.L.U. PRODUIT L'ANNEE

3.20. Remarque. L'ordre de Bruhat est donc encore une fois un *ordre de dégénérescence* d'orbites pour l'action d'un groupe topologique. Comme son nom l'indique, il a été introduit par Ehresmann en 1934 dans [25] et étendu par Chevalley pour les autres groupes classiques (et un peu plus) en 1958. Il en existe beaucoup d'autres descriptions, par exemple en termes de sous-mots de décompositions réduites comme produit des générateurs $(i,i+1)$ $(1 \leqslant i \leqslant n-1)$, voir [10].

Démonstration. Il suffit de montrer que (i) est équivalent à (ii).

Notons $G = \mathrm{GL}_n(\mathbb{K})$. Supposons que $\mathscr{C}_{\sigma'} \subset \overline{\mathscr{C}_\sigma}$. En résumé, pour montrer (ii), il suffit de regarder l'image des drapeaux dans la grassmannienne.

Détaillons. Fixons m entre 1 et n et considérons le diagramme suivant, où les flèches verticales, qui désignent les applications orbitales $gB \mapsto g \cdot F_\bullet^{\mathrm{std}}$ et $gP_k \mapsto g \cdot F_m^{\mathrm{std}}$, sont des homéomorphismes :

$$\begin{array}{ccc} & G & \\ {\scriptstyle\pi}\swarrow & & \searrow{\scriptstyle\pi_m} \\ G/B & \xrightarrow[\varpi_m]{} & G/P_m \\ \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} \\ \mathscr{B} & \longrightarrow & \mathrm{Gr}_{m,n}(\mathbb{K}) \end{array}$$

Comme P_m contient B, l'application $\varpi_m : G/B \to G/P_m$ est bien définie et continue ; comme π_m est ouverte, ϖ_m l'est aussi (vérifier !). Identifions quotients de groupe et espaces homogènes via les applications orbitales, qui sont des homéomorphismes, $G/B \to \mathscr{B}$, $gB \mapsto g \cdot F_\bullet^{\mathrm{std}}$ et

$G/P_m \to \mathrm{Gr}_{m,n}(\mathbb{K})$, $gP_k \mapsto g\cdot F_m^{\mathrm{std}}$. On notera encore $\varpi_m : \mathscr{B} \to \mathrm{Gr}_{m,n}(\mathbb{K})$ l'application correspondante : elle est ouverte et continue, par construction de la topologie sur la grassmannienne [H2G2, définition II-4.3.4].

Ainsi, l'image d'un drapeau de type σ' dans la grassmannienne appartient à l'adhérence de l'image de $\mathscr{C}_\sigma$. Or, l'image d'un drapeau $gF_\bullet^{\mathrm{std}}$ dans G/P_m est gF_m^{std}. Le type dans $\mathrm{Gr}_{m,n}(\mathbb{K})$ de $gF_\bullet^{\mathrm{std}}$ est donc $(i_1,\dots,i_m)$ de sorte que $\{i_1,\dots,i_m\} = \{\sigma(1),\dots,\sigma(m)\}$, de même pour σ'. Par [H2G2, proposition IV-3.6.1], qui décrit l'adhérence des cellules dans la grassmannienne, on a donc : $i'_1 \leqslant i_1,\dots,i'_m \leqslant i_m$.

Réciproquement, supposons les conditions de (ii) réalisées. Pour montrer que l'on a : $\mathscr{C}_{\sigma'} \subset \overline{\mathscr{C}_\sigma}$, il suffit de montrer qu'un élément particulier de $\mathscr{C}_{\sigma'}$ appartient à l'adhérence de $\mathscr{C}_\sigma$. En effet, $\mathscr{C}_{\sigma'}$ est une orbite sous B et l'adhérence de $\mathscr{C}_\sigma$, en tant qu'adhérence d'orbite, est stable sous B.

Pour t scalaire non nul, posons : $A(t) = t\sigma + \sigma'$. Pour t différent de 0 et -1, le pivot de la colonne j est sur la ligne $\sigma(i)$ $(1 \leqslant j \leqslant n)$ donc $A(t)$ appartient à $B\sigma B$. Lorsque t tend vers 0, $A(t)$ tend vers σ', élément de $B\sigma' B$. Par suite, $A(t)\cdot F_\bullet^{\mathrm{std}}$ appartient à $\mathscr{C}_\sigma$ et tend vers un élément de $\mathscr{C}_{\sigma'}$ lorsque t tend vers 0. L'inclusion de $\mathscr{C}_{\sigma'}$ dans l'adhérence de $\mathscr{C}_\sigma$ en résulte. □

3.21. Exemple. Reprenons l'exemple 3.12. On peut y voir que l'orbite $B(13)B$ dégénère sur l'orbite $B(123)B$ et sur l'orbite $B(132)B$.

On peut en effet remarquer que (123) et (132) sont plus petits que (13) pour l'ordre de Bruhat.

3.22. Corollaire. *Soit w_0 de $\mathfrak{S}_n$ tel que $w_0(i) = n - i + 1$ pour tout i. Alors, on a : $\overline{\mathscr{C}_{w_0}} = G/B$.*

Démonstration. On voit (exercice A.13) que par définition de l'ordre de Bruhat, w_0 est le plus grand élément de $\mathfrak{S}_n$. L'assertion en résulte. □

3.23. Remarque (Les groupes B et W). Si l'on note B le groupe des matrices inversibles triangulaires supérieures et W le groupe des matrices de permutation, la décomposition de Bruhat s'écrit :

$$\mathrm{GL}_n(\mathbb{K}) = BWB.$$

Le groupe B possède des caractérisations relevant de champs différents :
- groupe des matrices triangulaires supérieures (utiles pour l'algorithme de Gauss, caractérisation « linéaire algébrique »),
- sous-groupe minimal parmi les sous-groupes fermés H de $\mathrm{GL}_n(\mathbb{K})$ pour lesquels $\mathrm{GL}_n(\mathbb{K})/H$ est compact (caractérisation « géométrique »),
- sous-groupe connexe[9] résoluble maximal de $\mathrm{GL}_n(\mathbb{K})$ (caractérisation « algébrique », voir et amender [H2G2, exercice IV-B.3]).

[9] Cela a au moins un sens sur $\mathbb{R}$ et $\mathbb{C}$.

Les deux dernières propriétés ont un sens si l'on remplace $\mathrm{GL}_n(\mathbb{K})$ par un autre groupe classique et restent équivalentes. On donne le nom de *sous-groupes de Borel*[10] à ces sous-groupes, ils jouent un rôle éminent dans la théorie des représentations des groupes classiques.

Dans $\mathrm{GL}_n(\mathbb{K})$, le sous-groupe B possède un sous-groupe nilpotent maximal U, comme *unipotent* : le groupe des matrices triangulaires supérieures ayant pour seule valeur propre 1. Lorsque $\mathbb{K}$ est un corps fini, U est un sous-groupe de Sylow de $\mathrm{GL}_n(\mathbb{K})$ ([H2G2, proposition VIII-1.4]). Le sous-groupe U est distingué dans B et on a un isomorphisme : $B = U \rtimes T$, où T est le groupe des matrices diagonales. Le quotient du normalisateur N de T (le sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ formé des matrices ayant un seul coefficient non nul par ligne et par colonne) par T est isomorphe à W. Le paragraphe 5 détaille cette approche.

Si l'on remplace $\mathrm{GL}_n(\mathbb{K})$ par un groupe classique G, le paragraphe précédent a un sens (hormis les parenthèses) et la décomposition de Bruhat reste valable : $G = BWB$. On peut l'interpréter comme un substitut de l'algorithme de Gauss pour des contextes plus généraux.

Dites-moi, vous, on ne vous a pas entendu. On ne vous entend jamais. Vous n'arrêtez pas de bavarder. Faites attention, faites très attention.

4. Caractérisation algébrique des cellules de Schubert

Les représentations fondamentales de $\mathrm{GL}_n(\mathbb{K})$ vont nous permettre de caractériser les cellules et les variétés de Schubert à l'aide de relations algébriques que nous allons voir, valables sur tout corps. On note toujours $G = \mathrm{GL}_n(\mathbb{K})$, où $\mathbb{K}$ est un corps quelconque, et B le sous-groupe des matrices triangulaires supérieures de G.

Pour tout m de $[1, n-1]$, on considère l'ensemble $\Lambda(m,n)$ ordonné par la relation $\preceq_m$ définie en 3.17. Pour tout I dans $\Lambda(m,n)$, on pose $\Delta_I = \Delta_{I,I_m}$, où $I_m = [1,m]$. Pour tout σ de $\mathfrak{S}_n$, soit $\mathscr{B}_\sigma$ la partie de la variété des drapeaux $\mathscr{B} = G/B$ définie par

$$\mathscr{B}_\sigma = \{\overline{g} \in G/B,\ \Delta_I(g) = 0,\ I \not\preceq_m \sigma(I_m),\ \forall I \in \Lambda(m,n)\}$$

Il n'est pas totalement clair que l'égalité $\Delta_I(g) = 0$ ci-dessus ne dépend pas du représentant g choisi. Nous le montrons, entre autres, dans la proposition qui suit, qui caractérise algébriquement les variétés de Schubert ainsi que les cellules de Schubert.

[10] Ces sous-groupes portent le nom d'Armand Borel (1923-2003), mathématicien suisse.

4.1. Proposition. *Pour tout σ de $\mathfrak{S}_n$, la variété $\mathscr{B}_\sigma$ est la réunion de cellules $\bigcup_{\sigma' \preceq \sigma} B\sigma' B$. De plus, la cellule $\mathscr{C}_\sigma = B\sigma B$ est caractérisée, dans $\mathscr{B}_\sigma$, par*

$$\mathscr{C}_\sigma = \{\overline{g} \in \mathscr{B}_\sigma,\ \Delta_{\sigma(I_m)}(g) \neq 0,\ \forall m \in [1, m-1]\}$$

Démonstration. Tout d'abord, notons les faits simples suivants. Si $b = (b_{ij})$ est inversible et triangulaire supérieure, alors b_{ii} est non nul pour tout i. Pour tout m de $[1, n-1]$, le mineur $\Delta_{I,J}(b)$ est nul dès que $I \not\preceq_m J$. En effet, par définition de l'ordre $\preceq_m$, la « non-inégalité » implique que les $m!$ termes du développement du déterminant sont nuls. En particulier, $\Lambda^m(b)$ est une matrice triangulaire supérieure inversible, donc avec des termes non nuls sur la diagonale.

Comme I_m est la plus petite partie de $\Lambda(m,n)$ pour $\preceq_m$, la formule de Binet, voir théorème 1.2, nous donne que si g vérifie $\Delta_I(g) = \Delta_{I,I_m}(g) = 0$, alors $\Delta_I(gb) = 0$. La relation $\Delta_I(g)$ passe donc bien au quotient de G/B.

De plus, si $\overline{g} \in \mathscr{B}_\sigma$, alors pour tout I, $I \not\preceq \sigma(I_m)$, on a, pour tout b de B :

$$\begin{aligned}\Delta_{I,I_m}(bg) &= \sum_K \Delta_{I,K}(b)\Delta_{K,I_m}(g) \\ &= \sum_{I \preceq_m K} \Delta_{I,K}(b)\Delta_{K,I_m}(g) \\ &= \sum_{I \preceq_m K} \Delta_{I,K}(b) \times 0 = 0.\end{aligned}$$

Cela implique que $\mathscr{B}_\sigma$ est une réunion de B-orbites pour l'action à gauche de B sur G/B.

Par la décomposition de Bruhat, voir le théorème 3.11, les représentants de ces orbites sont les classes de matrices de permutation ; la première assertion se ramène à montrer $\overline{\sigma'} \in \mathscr{B}_\sigma \Leftrightarrow \sigma' \preceq \sigma$.

Or, par l'exercice 1.15, on a :

$$\Delta_I(\sigma') = \pm\delta_{I,\sigma'(I_m)},$$

où δ est le symbole de Kroenecker. Il en résulte que $\overline{\sigma'} \in \mathscr{B}_\sigma$ si et seulement si $\sigma'(I_m) \preceq_m \sigma(I_m)$ pour tout m, c'est-à-dire si et seulement si $\sigma' \preceq \sigma$.

Reste à montrer la seconde assertion. Par la formule de Binet 1.2, on voit encore que la condition $\Delta_{\sigma(I_m)}(g) \neq 0$, pour $\overline{g} \in \mathscr{B}_\sigma$, passe au double quotient (à droite et à gauche) dans $B\backslash G/B$ et on se ramène donc à montrer que $\Delta_{\sigma(I_m)}(\sigma') \neq 0$ pour tout $m \in [1, m-1] \Leftrightarrow \sigma = \sigma'$, ce qui résulte du calcul de $\Delta_I(\sigma')$ ci-dessus. □

4.2. Exercice. *Vérifier le résultat de l'exemple 3.12 à l'aide de la proposition 4.1.*

4.3. Remarque. En particulier, si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, la cellule $B\sigma B$ est un ouvert dense de la variété algébrique $\mathscr{B}_\sigma$. À l'instar des actions topologiques étudiées dans le tome premier, l'action de B sur la variété des drapeaux G/B possède des orbites localement fermées, *i.e.* ouvertes dans leur adhérence. On appelle les cellules $B\sigma B$ *cellules de Schubert* et *variétés de Schubert* les adhérences $\mathscr{B}_\sigma$ (ce sont des variétés algébriques, singulières en général).

Voici une application facile de cette caractérisation algébrique à un résultat bien connu et si général qu'il s'en trouve même axiomatisé dans le cadre des BN-paires dues à Tits. Notons toutefois que la proposition 4.1 n'est pas absolument nécessaire à la preuve et que tout disciple de l'algorithme de Gauss se gausserait de voir utiliser la formule de Binet pour une chose somme toute presque benête.

4.4. Définition. On appelle *transposition simple*, une transposition de la forme $(i, i+1)$.

4.5. Corollaire. *Soient u une permutation et s la transposition simple $(i, i+1)$ de $\mathfrak{S}_n$ vues comme matrices de permutations de $G = \mathrm{GL}_n(\mathbb{C})$.*

Alors, on a : $sBu \subset BsuB \cup BuB$.

Plus précisément, pour $b \in B$,

$$sbu \in \begin{cases} BuB & \text{si } \Delta_{su(I_m),u(I_m)}(b) \neq 0 \text{ pour } m \in [1, n-1], \\ BsuB & \text{sinon.} \end{cases}$$

En particulier, si $u \preceq su$, c'est-à-dire si $u^{-1}(i) < u^{-1}(i+1)$, alors $sBu \subset BsuB$. Si $su \preceq u$, c'est-à-dire si $u^{-1}(i) > u^{-1}(i+1)$, et $b \in B$, alors $sbu \subset BuB$ si $b_{i,i+1} \neq 0$ et $sbu \subset BsuB$ sinon.

Démonstration. Tout d'abord, on remarque que, vu que s permute uniquement deux éléments, et que ceux-ci sont consécutifs pour l'ordre naturel, on a la propriété, pour toutes parties I, J de $\Lambda^{(m,n)}$:

$$\text{si } I \not\preceq J \text{ et } s(I) \preceq s(J), \text{ alors, } I = s(J); \tag{1}$$

$$\text{si } I \not\preceq J \text{ et } s(I) \preceq J, \text{ alors, } I = s(J). \tag{2}$$

Soit b dans B. La formule de Binet donne, avec l'exercice 1.15,

$$\Delta_I(bu) = \sum_K \Delta_{I,K}(b)\Delta_{K,I_m}(u) = \sum_K \Delta_{I,K}(b)\varepsilon\delta_{K,u(I_m)} = \varepsilon\Delta_{I,u(I_m)}(b),$$

où $\varepsilon = \pm 1$. Cela donne, avec $\varepsilon' = \pm 1$:

$$\Delta_I(sbu) = \sum_K \Delta_{I,K}(s)\Delta_K(bu) = \sum_K \varepsilon\varepsilon'\delta_{I,s(K)}\Delta_{K,u(I_m)}(b)$$

$$\Delta_I(sbu) = \varepsilon\varepsilon'\Delta_{s(I),u(I_m)}(b). \tag{3}$$

Or, le mineur $\Delta_{I,J}(b)$ est nul si $I \not\geq_m J$ et non nul si $I = J$.

Par la propriété 1, si $I \not\preceq su(I_m)$ et $I \neq u(I_m)$, alors $s(I) \not\preceq u(I_m)$ d'où, par 3 : $\Delta_I(sbu) = 0$. De plus, on a : $\Delta_{su(I_m)}(sbu) = \Delta_{s(I),u(I_m)}(b) \neq 0$.

Premier cas. Si $u \preceq su$. Dans ce cas, $I \not\preceq su(I_m)$ implique $I \neq u(I_m)$, et donc par la proposition 4.1, $sbu \in BsuB$.

Second cas. Si $su \preceq u$. Supposons $I \not\preceq u(I_m)$. Alors, nécessairement, $I \neq su(I_m)$, et donc $s(I) \not\preceq u(I_m)$ par 2, et donc $\Delta_I(sbu) = 0$. Cela implique $sbu \in \bigcup_{u' \preceq u} Bu'B$ par la proposition 4.1.

Si $\Delta_{su(I_m),u(I_m)}(b) \neq 0$ pour tout m de $[1, n-1]$, alors $\Delta_{u(I_m)}(sbu) \neq 0$ et dans ce cas, $sbu \in BuB$ par la proposition 4.1.

Sinon, alors par la même proposition, $sbu \notin BuB$. Soit u_0 tel que $sbu \in Bu_0B$, on a alors d'après ce qui précède que $u_0 \neq u$ et $su \preceq u_0 \preceq u$. Cela implique, par exemple par un argument de longueur tiré de la proposition A.9, que $u_0 = su$. Et donc : $sbu \in BsuB$.

Pour finir, on remarque que dans ce second cas, $u(I_m)$ et $su(I_m)$ ne diffèrent éventuellement que si $i+1 \in u(I_m)$ et $i \in su(I_m)$ et le cas échéant, on a $su(I_m) = u(I_m) \setminus \{i+1\} \cup \{i\}$. Cela prouve facilement en développant un mineur que la condition $\Delta_{su(I_m),u(I_m)}(b) \neq 0, \forall m \in [1, n-1]$ est équivalente à $b_{i,i+1} \neq 0$. □

4.6. Remarque. Le fait que $\Delta_{su(I_m),u(I_m)}(b) \neq 0$ pour tout $m \in [1, n-1]$ ne dépend pas de u, mais seulement de b. Il est équivalent de dire que $b_{i,i+1} \neq 0$ ou encore que $sbs^{-1} \notin B$.

4.7. Corollaire. *Soit s_k la transposition simple $(k, k+1)$. Alors,*

(i) *L'ensemble $P_k = Bs_kB \cup B$ est un sous-groupe de G.*

(ii) *Tout sous-groupe de G contenu dans P_k et contenant strictement B est égal à P_k.*

(iii) *Si pour un élément u de $\mathfrak{S}_n$, on a : $u \preceq s_ku$, alors l'intersection de P_k/B avec la variété de Schubert $\mathscr{B}_u$ est égale à B.*

Démonstration. Le point (i) provient directement du corollaire 4.5.

Si un sous-groupe H de G est contenu dans P_k et contient strictement B, il contient bs_kb', pour b, b' dans B, et donc s_k. Il contient donc $Bs_kB \cup B = P_k$. Cela donne le point (ii).

Le point (iii) découle directement de la décomposition de Bruhat, voir théorème 3.11. □

4.8. Définition. Un *sous-groupe parabolique* de $G = \mathrm{GL}_n(\mathbb{K})$ est un sous-groupe de G contenant B ou un conjugué de B. Les P_k $(1 \leqslant k \leqslant n-1)$, sont des *sous-groupes paraboliques minimaux.*

En calculant directement bs_kb', pour $b, b' \in B$, on voit facilement que P_k est constitué des matrices (p_{ij}) telles que $p_{ij} = 0$, pour tout couple (i,j), $p_{i,j} = 0$ dès que $i > j$ et $(i,j) \neq (k+1,k)$.

Écoutez, j'ai une conception personnelle de l'ouvrage.
Ce n'est pas assez triomphal, pas assez orgueilleux.

5. BN-paire et algèbre de Hecke

Cette partie poursuit l'exploration de la décomposition de Bruhat en mettant plus en évidence son interaction avec la combinatoire du groupe symétrique. Non triviale, elle reste cependant élémentaire, au sens où il n'y a ni déterminant ni géométrie algébrique cachée. On commence par prouver à nouveau le corollaire 4.5 avec moins de déterminants. Puis, on « abstrait » cette propriété dans le système d'axiomes qui décrit les *BN-paires*, et qui permet d'étendre la décomposition de Bruhat aux autres groupes classiques. On utilisera cette structure pour définir la belle *algèbre de Hecke*, dont on évoquera l'intérêt et que l'on retrouvera bien plus tard, au moment de la théorie des représentations.

La partie qui concerne la BN-paire est tirée du livre de Meinolf Geck [33].

5.1. Notations. On fixe un entier naturel n et un corps $\mathbb{K}$. On note comme précédemment B le sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ formé des matrices triangulaires supérieures, mais aussi T le groupe des matrices diagonales, U le sous-groupe de B formé des matrices triangulaires unipotentes (les coefficients diagonaux valent 1).

Si i et j sont deux entiers distincts compris entre 1 et n, on note E_{ij} la matrice élémentaire dont le seul coefficient non nul est en position (i,j) et X_{ij} le groupe des matrices de la forme $\mathrm{I}_n + \lambda E_{ij}$, $\lambda \in \mathbb{K}$. Si $1 \leqslant i \leqslant n-1$, on note $X_i = X_{i,i+1}$ et $X_{-i} = X_{i+1,i}$. Enfin, on appelle V_i le sous-groupe de B formé des matrices dont le coefficient d'indice $(i, i+1)$ vaut 0. On vérifie qu'il s'agit bien d'un sous-groupe par un calcul matriciel par blocs.

On conserve les notations relatives au groupe symétrique $\mathfrak{S}_n$ que l'on identifie au groupe W des matrices de permutations : autrement dit, pour un élément $w \in \mathfrak{S}_n$, on note également w la matrice $n \times n$ dont le coefficient d'indice (i,j) est : $\delta_{i,w(j)}$ (le delta de Kronecker).

5.2. Lemme

(i) *Le sous-groupe U est distingué dans B. De plus :*

$$B = UT = TU, \quad T \cap U = \{\mathrm{I}_n\}.$$

En particulier, B est isomorphe au produit semi-direct $U \rtimes T$, où T agit sur U par conjugaison.

(ii) *Si $\mathbb{K}$ possède au moins trois éléments, le normalisateur N de T dans $\mathrm{GL}_n(\mathbb{K})$ est le groupe des matrices monomiales (un coefficient non nul par ligne et par colonne) inversibles.*

Démonstration. (i) Le fait que U est distingué se vérifie facilement : l'application qui, à une matrice triangulaire de B, associe sa diagonale dans $\mathbb{K}^{*n}$ est un morphisme dont U est le noyau. Soit $g \in B$, notons $\lambda_1, \ldots, \lambda_n$ ses coefficients diagonaux et $h \in T$ la matrice qui a la même diagonale que g. On vérifie que $h^{-1}g$ et gh^{-1} appartiennent à U. Cela entraîne les égalités $B = TU = UT$. L'égalité $T \cap U = \{\mathrm{I}_n\}$ est évidente. Cela précède montre que la projection canonique $B \to B/U$ se restreint en un isomorphisme $T \to B/U$, et ce qui assure que B est isomorphe à $U \rtimes T$, [H2G2, proposition II-5.8].

(ii) Soit $g \in N$. Soient $k \in \{1, \ldots, n\}$ et μ deux scalaires non nuls distincts. Posons $h_k = \lambda \mathrm{I}_n + (\mu - \lambda)E_{k,k}$. Fixons i dans $\{1, \ldots, n\}$. Par principe de conjugaison, l'espace propre associé à la valeur propre μ de gh_kg^{-1} est la droite $\mathbb{K}g(e_i)$, où e_i est le i-ème vecteur de la base canonique. Mais comme la matrice gh_ig^{-1} est diagonale, elle commute à tous les h_k $(1 \leqslant k \leqslant n)$, donc h_k préserve les espaces propres de gh_ig^{-1}. Autrement dit, $g(e_i)$ est un vecteur propre de tous les h_k. Cela signifie que $g(e_i)$ est sur la droite $\mathbb{K}e_k$ ou dans l'hyperplan de coordonnées $H_k = \bigoplus_{j \neq k} \mathbb{K}e_j$. Si $g(e_i)$ appartient à n hyperplans H_k de coordonnées, alors, il est nul, ce qui est absurde. On en déduit que $g(e_i)$ est de la forme $\lambda_i e_{w(i)}$, pour un $w(i) \in \{1, \ldots, n\}$. Comme cela est vrai pour tout i, w est nécessairement une permutation. Mais alors, $w^{-1}g$ est diagonale et g est monomiale. ¡Que pesadez! □

On va utiliser les sous-groupes V_i et X_i définis en début de section.

5.3. Lemme

(i) *Soient $1 \leqslant i \leqslant n-1$, on a : $U = V_iX_i = X_iV_i$.*

(ii) *Soient $w \in \mathfrak{S}_n$ et $1 \leqslant i, j \leqslant n$ avec $i \neq j$, on a : $wX_{ij}w^{-1} = X_{w(i),w(j)}$.*

(iii) *Soit $1 \leqslant i \leqslant n-1$, on a : $s_iX_is_i^{-1} = X_{-i}$ et $s_iV_is_i^{-1} = V_i$.*

Démonstration. Pour l'assertion (i), fixons $g \in U$ et soit λ le coefficient d'indice $(i, i+1)$ de g. Posons $h = \mathrm{I}_n - \lambda E_{i,i+1} \in X_i$. On vérifie que gh et hg appartiennent tous deux à V_i, ce qui entraîne que $g \in V_iX_i$ et $g \in X_iV_i$.

Les assertions (ii) et (iii) sont des avatars du principe de conjugaison. □

5.4. Proposition. *Soient $i \in \{1, \dots, n-1\}$ et $w \in \mathfrak{S}_n$. On a :*

$$s_i B w \subset B s_i w B \cup B w B.$$

Démonstration. On commence par le cas où $w = s_i$. On a, pour $\lambda \neq 0$:

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}.$$

Dans $\mathrm{GL}_2(\mathbb{K})$, il vient : $X_{-1} \setminus \{\mathrm{I}_2\} \subset X_1 s_1 X_1 T$ et : $X_{-1} \subset \{\mathrm{I}_2\} \cup X_1 s_1 X_1 T$. Passons dans $\mathrm{GL}_n(\mathbb{K})$ grâce au morphisme

$$\begin{array}{rccc} \varphi_i : & \mathrm{GL}_2(\mathbb{K}) & \longrightarrow & \mathrm{GL}_n(\mathbb{K}) \\ & h & \longmapsto & \begin{pmatrix} \mathrm{I}_{i-1} & & \\ & h & \\ & & \mathrm{I}_{n-i-1} \end{pmatrix}. \end{array}$$

Comme φ_i envoie le X_{-1} de $\mathrm{GL}_2(\mathbb{K})$ sur le X_{-i} de $\mathrm{GL}_n(\mathbb{K})$, etc., on a :

$$X_{-i} V_i \subset (V_i) \cup (X_i s_i X_i T V_i) \subset B \cup B s_i B.$$

On prend désormais w quelconque et on distingue deux cas. On suppose d'abord que $w^{-1}(i) < w^{-1}(i+1)$. Alors, grâce au lemme 5.3 : $w^{-1} X_i w = X_{w^{-1}(i), w^{-1}(i+1)} \subset U$, ce qui donne : $X_i w \subset wU \subset wB$. On calcule de plus :

$$s_i B w = s_i V_i X_i T w = V_i s_i X_i w T \subset B s_i w B,$$

puisque $V_i \subset B$ et que $X_i w T \subset wBT = wB$.

Supposons à présent que $w^{-1}(i) > w^{-1}(i+1)$. Alors on pose $y = s_i w$, de sorte que l'on a : $y^{-1}(i) < y^{-1}(i+1)$. D'après ce qui précède, on peut écrire : $s_i B y \subset B s_i y B = BwB$, d'où :

$$s_i B w = s_i B s_i y \subset B y \cup B s_i B y \subset B s_i w \cup BwB \subset B s_i w B \cup BwB. \quad \square$$

On donne une version abstraite de ces propriétés.

5.5. Définition (Tits). Soit G un groupe. On dit que G admet une *BN-paire* ou un *système de Tits* s'il existe des sous-groupes B et N de G tels que :

(BN1) le groupe G est engendré par B et N ;

(BN2) le groupe $T = B \cap N$ est distingué dans N et le quotient $W = N/T$ est engendré par un ensemble S d'éléments d'ordre 2 ;

(BN3) pour s un représentant d'un élément de S dans N, on a : $sBs \neq B$;

(BN4) pour s un représentant d'un élément de S dans N et $w \in N$, on a : $sBw \subset BswB \cup BwB$;

(BN5) on a : $\bigcap_{w \in N} wBw^{-1} = T$.

5.6. Remarque. Les conditions qui définissent une BN-paire sont très contraignantes. En effet, elles suffisent pour montrer[11] que B est son propre normalisateur (1.6.4), que l'on a une sorte de décomposition LU (1.6.6) et même une décomposition de Bruhat, c'est-à-dire que $G = BWB$ (1.6.3), et que le lemme d'échange A.15 est vrai dans W (1.6.8). En particulier, l'intérêt d'une décomposition de Bruhat a été signalé dans la remarque 3.15.

5.7. Proposition. *Avec les notations 5.1, B et N forment une BN-paire dans le groupe* $\mathrm{GL}_n(\mathbb{K})$.

Démonstration. Comme B contient les transvections $\mathrm{I}_n + \lambda E_{ij}$ ($\lambda \in \mathbb{K}$ et $1 \leqslant i < j \leqslant n$) N contient les matrices de permutations, le groupe engendré par B et N contient aussi toutes les transvections $\mathrm{I}_n + \lambda E_{ij}$ ($i \neq j$ quelconques) et la propriété (BN1) résulte de l'algorithme du pivot de Gauss[12].

Une matrice monomiale et triangulaire est bien diagonale, d'où : $T = B \cap N$. On a vu que T est distingué dans son normalisateur N le quotient est isomorphe à $\mathfrak{S}_n$, qui d'après A.1 est engendré par les transpositions $s_i = (i, i+1)$ ($1 \leqslant i \leqslant n-1$). D'où (BN2).

Pour montrer (BN3), il suffit de remarquer que $s_i(\mathrm{I}_n + E_{i,i+1})s_i$ n'appartient pas à B. Quant à (BN4), c'est l'objet de la proposition 5.4.

Reste à montrer (BN5). Soit $w \in N$. Un élément g appartient à wBw^{-1} si et seulement s'il préserve l'image du drapeau standard par w. En particulier, le vecteur $w(e_1)$ est propre pour g. Mais dans N, on trouve toutes les matrices de permutations, si bien que si g appartient à tous les wBw^{-1}, alors tous les vecteurs de la base canonique sont propres pour g. Autrement dit, g appartient à T. L'inclusion de T dans l'intersection est évidente. □

5.8. Corollaire. *Pour toute réflexion simple s, on a : $BsBsB = BsB \cup B$, et c'est un sous-groupe de* $\mathrm{GL}_n(\mathbb{K})$.

Démonstration. Par la proposition 5.4, on sait que $sBs \subset BsB \cup B$, si bien que $BsBsB$ est une partie bi-invariante sous B, c'est-à-dire une réunion de double-classes, contenue dans $BsB \cup B$; elle contient B et, par la proposition 5.7 (l'axiome (BN3)), on sait que $sBs \neq B$, si bien que $BsBsB = BsB \cup B$. Cela entraîne la stabilité de $BsB \cup B$ par produit et la stabilité par passage à l'inverse vient de ce que s est une involution. □

La structure de BN-paire suffit à établir la décomposition de Bruhat. Suivant [33, Proposition 1.6.3], on retrouve de façon abstraite un résultat établi deux fois.

[11] Les numéros entre parenthèses se réfèrent à [33] où l'on trouve les preuves.

[12] Il semble possible d'expliquer tout l'univers par le *big bang* et l'algorithme de Gauss.

5.9. Corollaire. *On a une réunion disjointe :* $G = \bigcup_{w \in W} BwB$.

Comme application de la notion de BN-paire, nous définissons l'*algèbre de Hecke* (en plusieurs versions). Pour l'instant, l'exercice semble gratuit mais nous la retrouverons plus tard via les représentations de $\mathrm{GL}_n(\mathbb{F}_q)$.

5.10. Définition. Soit n un entier naturel non nul et soit $\mathbb{F}_q$ un corps fini à q éléments. On note $G = \mathrm{GL}_n(\mathbb{F}_q)$ et B le sous-groupe de G formé des matrices triangulaires, etc. On appelle *algèbre d'Iwahori-Hecke* ou *algèbre de Hecke* et on note $\mathscr{H}_n(q)$ l'espace des fonctions de G dans $\mathbb{Q}$ qui sont bi-invariantes sous B :

$$\mathscr{H}_n(q) = \big\{\phi : G \to \mathbb{Q},\ \forall g \in G,\ \forall b_1, b_2 \in B,\ \phi(b_1^{-1} g b_2) = \phi(g)\big\},$$

muni du produit de convolution défini pour $\phi_1, \phi_2 \in \mathscr{H}_n(q)$ par :

$$\forall g \in G, \quad \phi_1 * \phi_2(g) = \frac{1}{|B|} \sum_{g_1 g_2 = g} \phi_1(g_1)\phi_2(g_2),$$

où la somme porte sur les couples $(g_1, g_2) \in G \times G$ tels que $g = g_1 g_2$.

5.11. Lemme. *L'algèbre $\mathscr{H}_n(q)$ est une $\mathbb{Q}$-algèbre associative et unitaire. Elle admet pour base la famille $(\mathbf{T}_w)_{w \in \mathfrak{S}_n}$ des fonctions caractéristiques des double-classes BwB, $w \in \mathfrak{S}_n$.*

Démonstration. L'associativité résulte formellement de l'associativité du produit matriciel ; avec des notations évidentes, on a :

$$\begin{aligned}\phi_1 * (\phi_2 * \phi_3)(g) &= \frac{1}{|B|} \sum_{g_1 g' = g} \phi_1(g_1)(\phi_2 * \phi_3)(g') \\ &= \frac{1}{|B|^2} \sum_{g_1 g_2 g_3 = g} \phi_1(g_1)\phi_2(g_2)\phi_3(g_3),\end{aligned}$$

ce qui donne manifestement lieu à l'associativité.

L'unité est $\mathbf{T}_e$, la fonction caractéristique de B, puisque pour $\phi \in \mathscr{H}_n(q)$, on a :

$$\phi * \mathbf{T}_e(g) = \frac{1}{|B|} \sum_{g_1 g_2 = g} \phi(g_1)\mathbf{T}_e(g_2) = \frac{1}{|B|} \sum_{g_2 \in B} \phi(g g_2^{-1}) = \phi(g),$$

la dernière égalité résultant de l'invariance à droite : $\phi(g g_2^{-1}) = \phi(g)$ pour $g_2 \in B$. L'invariance à gauche donne de même $\mathbf{T}_e * \phi = \phi$.

Enfin, la bi-invariance montre qu'une fonction de $\mathscr{H}_n(q)$ est constante sur les double-classes, donc combinaison linéaire de leurs fonctions caractéristiques, lesquelles sont linéairement indépendantes puisque les double-classes forment une partition d'après le théorème 3.11 ou sa version abstraite 5.9.□

On a introduit dans l'annexe A.3, pour tout σ de $\mathfrak{S}_n$, la *longueur* $\ell(\sigma)$ de σ, qui mesure, en quelque sorte, la « distance » entre l'élément neutre e et σ, quand l'unité de mesure est la transposition simple.

5.12. Proposition. *Dans $\mathscr{H}_n(q)$, on a, pour $s \in S$ et $w \in \mathfrak{S}_n$ quelconques :*

$$\mathbf{T}_s * \mathbf{T}_w = \begin{cases} \mathbf{T}_{sw} & \text{si } \ell(sw) > \ell(w), \\ (q-1)\mathbf{T}_w + q\mathbf{T}_{sw} & \text{si } \ell(sw) < \ell(w). \end{cases}$$

Remarque. Lorsque $w = s$, on obtient en notant $\mathbf{T}_e = 1$:

$$\mathbf{T}_s * \mathbf{T}_s = (q-1)\mathbf{T}_s + q, \quad \text{ou encore :} \quad (\mathbf{T}_s - q) * (\mathbf{T}_s + 1) = 0.$$

Démonstration de la proposition. On commence par le cas où $w = s$. Tout d'abord, on a par le lemme 3.9 : $|BsB| = |BsB/B| \cdot |B| = q|B|$, d'où :

$$\mathbf{T}_s * \mathbf{T}_s(\mathrm{I}_n) = \frac{1}{|B|} \sum_{g_1 \in BsB} \mathbf{T}_s(g_1)\mathbf{T}_s(g_1^{-1}) = q.$$

Le corollaire 5.8 montre que le produit induit une surjection

$$F : BsB \times BsB \to BsB \cup B.$$

Cette application est compatible[13] avec l'action de $B \times B$ où (b_1, b_2) agit sur $(g_1, g_2) \in BsB \times BsB$ par $(b_1^{-1}g_1, g_2b_2)$ et sur $g \in BsB$ par $b_1^{-1}gb_2$. Comme cette dernière action est transitive, le cardinal d'une fibre $F^{-1}(g)$ ne dépend que de la double-classe à laquelle g appartient.

Ainsi, un élément de g de B possède, comme I_n, $|BsB| = q|B|$ antécédents (de la forme $(x, x^{-1}g)$ avec $x \in BsB$). Par suite, il reste $\big(q|B|\big)^2 - q|B| \cdot |B|$ éléments dans $BsB \times BsB$ qui s'envoient sur les $q|B|$ éléments de BsB ; autrement dit, chaque élément de BsB possède $(q-1)|B|$ antécédents. On a donc, pour $g \in BsB$:

$$\mathbf{T}_s * \mathbf{T}_s(g) = \frac{1}{|B|} \sum_{(g_1,g_2) \in F^{-1}(g)} \mathbf{T}_s(g_1)\mathbf{T}_s(g_2) = q - 1.$$

Comme $\mathbf{T}_s * \mathbf{T}_s(g) = 0$ si $g \notin BsB \cup B$, il vient : $\mathbf{T}_s * \mathbf{T}_s = (q-1)\mathbf{T}_s + q\mathbf{T}_e$.

À présent, soit w quelconque tel que $\ell(sw) > \ell(w)$. On connaît l'inclusion $sBw \subset BswB$ depuis la preuve de la proposition 5.4. Cela entraîne l'inclusion : $BsBwB \subset BswB$, et l'inclusion inverse est évidente. Le produit induit donc une surjection $\tilde{F} : BsB \times BwB \to BswB$; de plus, par bi-invariance, tous les éléments de $BswB$ possèdent le même nombre d'an-

[13] C'est-à-dire que $F((b_1, b_2) \cdot (g_1, g_2)) = (b_1, b_2) \cdot F(g_1, g_2)$.

técédents. Sachant que, par le lemme 3.9, on a :

$$|BsB| = q|B|, \quad |BwB| = q^{\ell(w)}|B| \quad \text{et} \quad |BswB| = q^{\ell(sw)}|B|,$$

ce nombre d'antécédents est exactement $|B|$. Il vient, pour $g \in BswB$:

$$\mathbf{T}_s * \mathbf{T}_w(g) = \frac{1}{|B|} \sum_{(g_1,g_2)\in\tilde{F}^{-1}(g)} \mathbf{T}_s(g_1)\mathbf{T}_w(g_2) = 1,$$

ce qui exprime que $\mathbf{T}_s * \mathbf{T}_w = \mathbf{T}_{sw}$.

Enfin, reste le cas où $\ell(sw) < \ell(w)$. On peut appliquer le résultat précédent à sw : $\mathbf{T}_s * \mathbf{T}_{sw} = \mathbf{T}_w$, ce qui donne :

$$\mathbf{T}_s * \mathbf{T}_w = \mathbf{T}_s * \mathbf{T}_s * \mathbf{T}_{sw} = \big((q-1)\mathbf{T}_s + q\mathbf{T}_e\big) * \mathbf{T}_{sw} = (q-1)\mathbf{T}_w + q\mathbf{T}_{sw}. \ \square$$

5.13. Corollaire. *Si $w = s_{i_1} \cdots s_{i_r}$ est une décomposition réduite de $w \in \mathfrak{S}_n$ avec $s_{i_1}, \ldots, s_{i_r} \in S$ et $r = \ell(w)$, on a dans $\mathscr{H}_n(q)$:*

$$\mathbf{T}_w = \mathbf{T}_{i_1} * \cdots * \mathbf{T}_{i_r}.$$

5.14. Remarque. Le corollaire montre en particulier que $\mathbf{T}_w$ ne dépend pas de la décomposition réduite, ce qui est vu d'habitude comme une conséquence facile d'une propriété non triviale appelée *lemme de Matsumoto.*

Démonstration. Puisque $\ell(s_{i_s} \cdots s_{i_r}) > \ell(s_{i_{s+1}} \cdots s_{i_r})$, il suffit d'appliquer $r-1$ fois la proposition dans le cas facile où la longueur augmente. $\square$

On rend q générique en constatant que les « constantes de structures » — les $c_{w,w'}^{w''}$ dans la proposition suivante — sont polynomiales. On fixe une indéterminée $\mathbf{q}$.

5.15. Proposition. *Il existe une unique famille de polynômes $c_{w,w'}^{w''}(\mathbf{q}) \in \mathbb{Q}[\mathbf{q}]$ $(w, w', w'' \in \mathfrak{S}_n)$ telle que pour tout q, puissance d'un nombre premier, on a dans $\mathscr{H}_n(\mathbb{F}_q)$:*

$$(\heartsuit) \qquad \forall w, w' \in \mathfrak{S}_n, \quad \mathbf{T}_w * \mathbf{T}_{w'} = \sum_{w''\in\mathfrak{S}_n} c_{w,w'}^{w''}(q)\mathbf{T}_{w''}.$$

Démonstration. Pour $w \in \mathfrak{S}_n$ fixé, les $c_{w,w'}^{w''}(q)$ sont les coefficients de la matrice de l'endomorphisme $\mathscr{H}_n(q) \to \mathscr{H}_n(q)$, $\phi \mapsto \mathbf{T}_w * \phi$ dans la base des $(\mathbf{T}_w)$. Lorsque $w = s \in S$, ce sont des polynômes en q d'après la proposition 5.12. Pour w quelconque, $\mathbf{T}_w$ est le produit de certains $\mathbf{T}_s$, $s \in S$ par le corollaire 5.13 donc les coefficients matriciels sont encore polynomiaux. L'unicité vient du fait qu'il existe une infinité de puissances de nombres premiers : les polynômes $c_{w,w'}^{w''}$ sont déterminés par leurs valeurs en ces points. $\square$

5.16. Corollaire. *Soit* $\mathbf{q}$ *une indéterminée. On définit sur le* $\mathbb{Q}(\mathbf{q})$*-espace vectoriel* $\mathscr{H}_n(\mathbf{q})$ *ayant pour base* $(\mathbf{T}_w)_{w\in\mathfrak{S}_n}$ *une opération bilinéaire* $*$ *par les formules* ($\heartsuit$)*. Alors, l'opération* $*$ *fait de* $\mathscr{H}_n(\mathbf{q})$ *une algèbre associative unitaire.*

Démonstration. L'associativité équivaut aux relations $\sum_{w',w''} c^{w'}_{w_1,w_2} c^{w''}_{w',w_3} = \sum_{w',w''} c^{w''}_{w_1,w'} c^{w''}_{w_2,w_3}$ pour tous $w_1, w_2, w_3 \in \mathfrak{S}_n$. Or, cette relation polynomiale est vraie puisqu'elle est satisfaite pour une infinité de valeurs de $\mathbf{q}$: les puissances d'un nombre premier. De même, le fait que $\mathbf{T}_e$ est neutre se traduit par les relations $c^{w'}_{w,e} = \delta_{w,w'} = c^{w'}_{e,w}$ (delta de Kronecker) pour tous $w, w' \in \mathfrak{S}_n$, relation vraie pour la même raison. □

5.17. Remarque. Soient $\mathbf{q}$ une indéterminée et q une puissance d'un nombre premier. L'application $\mathscr{H}_n(\mathbf{q}) \to \mathscr{H}_n(q)$, $\mathbf{q} \mapsto q$, $\mathbf{T}_w \mapsto \mathbf{T}_w$ est un morphisme de $\mathbb{Q}$-algèbres.

5.18. Lemme. *Soient* q *un nombre complexe non nul ou une indéterminée et* n *un entier naturel non nul. Dans* $\mathscr{H}_n(q)$*, on a les relations :*

$$\begin{cases} (\mathbf{T}_i - q)(\mathbf{T}_i + 1) = 0 & \text{pour tout } i \in \{1, \dots, n-1\}, \\ \mathbf{T}_i \mathbf{T}_{i+1} \mathbf{T}_i = \mathbf{T}_{i+1} \mathbf{T}_i \mathbf{T}_{i+1} & \text{pour tout } i \in \{1, \dots, n-2\}, \\ \mathbf{T}_i \mathbf{T}_j = \mathbf{T}_j \mathbf{T}_i & \text{pour tous } i, j \text{ tels que } |i-j| \geqslant 2. \end{cases}$$

Démonstration. On commence par le cas où q est le cardinal d'un corps fini. La première famille de relations sur $\mathbf{T}_i^2$ a été vue à la proposition 5.12. Pour les relations de tresses, il suffit de remarquer que l'on a :

$$\begin{cases} \mathbf{T}_i \mathbf{T}_{i+1} \mathbf{T}_i = \mathbf{T}_{s_i s_{i+1} s_i} = \mathbf{T}_{s_{i+1} s_i s_{i+1}} = \mathbf{T}_{i+1} \mathbf{T}_i \mathbf{T}_{i+1} & \text{si } i \leqslant n-2, \\ \mathbf{T}_i \mathbf{T}_j = \mathbf{T}_{s_i s_j} = \mathbf{T}_{s_j s_i} = \mathbf{T}_j \mathbf{T}_i & \text{si } |i-j| \geqslant 2, \end{cases}$$

d'après le corollaire 5.13 et la remarque qui le suit. □

Il y a mieux ! Ces relations fournissent une *présentation* de l'algèbre de Hecke $\mathscr{H}_n(q)$ par générateurs et relations.

5.19. Théorème. *Soient* q *un nombre complexe non nul ou une indéterminée et* n *un entier naturel non nul. L'algèbre de Hecke* $\mathscr{H}_n(q)$ *admet une présentation comme* $\mathbb{Q}(q)$*-algèbre par les générateurs* T_i *(*$1 \leqslant i \leqslant n-1$*) et les relations :*

$$\begin{cases} (T_i - q)(T_i + 1) = 0 & \text{pour tout } i \in \{1, \dots, n-1\}, \\ T_i T_{i+1} T_i = T_{i+1} T_i T_{i+1} & \text{pour tout } i \in \{1, \dots, n-2\}, \\ T_i T_j = T_j T_i & \text{pour tous } i, j \text{ tels que } |i-j| \geqslant 2. \end{cases}$$

Remarque. Lorsque $q = 1$, il doit être plus ou moins clair pour les personnes qui connaissent la notion que $\mathscr{H}_n(1)$ est l'algèbre du groupe symétrique $\mathbb{Q}[\mathfrak{S}_n]$; cela sera précisé et montré dans l'exercice X-F.21. On dit que $\mathscr{H}_n(q)$ est une *déformation*, ou *déformation quantique*, de $\mathbb{Q}[\mathfrak{S}_n]$.

Démonstration. Soit $\mathbb{H}_n$ l'algèbre définie par la présentation du théorème. Comme pour la présentation du groupe symétrique à la proposition B.7, il y a deux parties indépendantes. D'une part, on borne la dimension de l'algèbre $\mathbb{H}_n$ en exhibant une famille qui l'engendre linéairement. D'autre part, on montre que cette famille est libre grâce à un morphisme de $\mathbb{H}_n$ dans une algèbre concrète, les endomorphismes de $\mathscr{H}_n(q)$.

Première étape. On montre que la famille $(T_w)_{w\in\mathfrak{S}_n}$ engendre $\mathbb{H}_n$ comme espace vectoriel. Ici, on pose $T_e = 1$ et, pour $w \in \mathfrak{S}_n$, $w \neq e$, on note $w = s_{i_{n-1}} s_{i_{n-1}+1} \cdots s_{n-1}\, s_{i_{n-2}} s_{i_{n-2}+1} \cdots s_{n-2} \cdots s_{i_1} s_1$ sa forme normale comme dans le lemme B.9 et on pose[14] :

$$T_w = T_{i_{n-1}} T_{i_{n-1}+1} \cdots T_{n-1}\, T_{i_{n-2}} T_{i_{n-2}+1} \cdots T_{n-2} \cdots T_{i_1} \cdots T_1.$$

On procède par récurrence sur n, l'énoncé étant trivial si $n \leqslant 2$. Soit $n \geqslant 3$, on suppose que tout élément de $\mathbb{H}_{n-1}$ est combinaison linéaire des T_w pour $w \in \mathfrak{S}_{n-1}$ —noter qu'il y a un morphisme évident de $\mathbb{H}_{n-1}$ vers $\mathbb{H}_n$. Prouvons l'affirmation suivante : tout monôme $M = T_{i_1} \cdots T_{i_r}$ $(1 \leqslant i_k \leqslant n-1)$ peut s'écrire comme une somme de monômes où T_{n-1} apparaît une fois au plus. Supposons donc que T_{n-1} apparaisse au moins deux fois. Il existe donc M_1 et M_2, monômes en les T_i et M', monôme en $T_1, \ldots, T_{n-2}$ tels que $M = M_1 T_{n-1} M' T_{n-1} M_2$. Par hypothèse de récurrence, M' est somme de monômes où T_{n-2} apparaît au plus une fois. S'il n'apparaît pas, vu que T_{n-1} commute à T_j si $j \leqslant n-3$, on peut remplacer $T_{n-1} M' T_{n-1}$ par $T_{n-1}^2 M'$, puis T_{n-1}^2 par une somme de deux termes où T_{n-1} apparaît au plus une fois. Si T_{n-2} apparaît, on écrit $M' = M_1' T_{n-2} M_2'$, puis l'on remplace $T_{n-1} M' T_{n-1}$ par $M_1' T_{n-1} T_{n-2} T_{n-1} M_2'$ et enfin par $M_1' T_{n-2} T_{n-1} T_{n-2} M_2'$. Dans chaque monôme que l'on vient de produire dans chaque cas, on a strictement réduit le nombre d'occurrences de T_{n-1} par rapport à l'expression initiale, ce qui prouve l'affirmation.

Si T_{n-1} n'apparaît pas dans un monôme, on l'exprime comme combinaison linéaire des T_w grâce à l'hypothèse de récurrence[15]. Si T_{n-1} apparaît dans un monôme $M_1 T_{n-1} M_2$, où $M_1, M_2 \in \mathbb{H}_{n-1}$, on écrit M_1 comme combinaison linéaire de termes de la forme $T_{i_{n-2}} T_{i_{n-2}+1} \cdots T_{n-2} \cdots T_{i_1} T_1$. Pour chaque terme, si T_{n-2} n'intervient pas ($i_{n-2} = n-1$), alors on a :

[14] Il est convenu que si $i_k = k+1$, on omet le paquet correspondant.

[15] L'algèbre H engendrée par $T_1, \ldots, T_{n-2}$ dans $\mathbb{H}_n$ est un quotient de $\mathbb{H}_{n-1}$. Il n'importe pas ici de savoir si H et $\mathbb{H}_{n-1}$ sont isomorphes, ce qui résulte de la preuve complète.

$M_1 T_{n-1} M_2 = T_{n-1} M_1 M_2$. Sinon, on a :

$$M_1 T_{n-2} M_2 = T_{i_{n-2}} T_{i_{n-2}+1} \cdots T_{n-2} T_{n-1} T_{i_{n-3}} \cdots T_{n-3} \cdots T_1 M_2 .$$

On traite enfin ce qui apparaît à droite de T_{n-1} avec l'hypothèse de récurrence.

Deuxième étape. On montre que la famille $(T_w)_{w \in \mathfrak{S}_n}$ est libre. Comme les $\mathbf{T}_i$ satisfont aux relations de $\mathbb{H}_n$, l'application $T_i \mapsto \mathbf{T}_i *?$ qui, à un générateur T_i de $\mathbb{H}_n$ associe la multiplication par $\mathbf{T}_i$, se prolonge en un morphisme d'algèbres associatives $\rho : \mathbb{H}_n \to \mathrm{End}_{\mathbb{Q}(q)}(\mathscr{H}_n(q))$. D'après le lemme 5.13, $\rho(T_w)(\mathbf{T}_e) = \mathbf{T}_w$. Comme les $\mathbf{T}_w$ sont linéairement indépendants dans $\mathscr{H}_n(q)$ (ce sont des fonctions caractéristiques sur des parties disjointes !), il en résulte que les T_w le sont dans $\mathbb{H}_n$: si $\sum_{w \in \mathfrak{S}_n} c_w T_w = 0$ dans $\mathbb{H}_n$, avec $c_w \in \mathbb{Q}(q)$ pour tout w, alors on a : $0 = \sum_{w \in \mathfrak{S}_n} c_w \rho(T_w)(\mathbf{T}_e) = \sum_{w \in \mathfrak{S}_n} c_w T_w$. Ainsi, tous les c_w sont nuls. On voit au passage que ρ est injectif.

On a montré que $\mathbb{H}_n$ admet la famille $(T_w)_{w \in \mathfrak{S}_n}$ comme base sur $\mathbb{Q}(q)$: sa dimension est donc $n!$. D'après la définition d'une présentation et le lemme 5.18, l'application $T_i \mapsto \mathbf{T}_i$ $(1 \leqslant i \leqslant n-1)$ induit un morphisme surjectif $\mathbb{H}_n \to \mathscr{H}_n(q)$. Par égalité des dimensions, c'est un isomorphisme.□

De l'orgueil, bon sang !
Papapan papan papan papapan tchac !
Papapan papan papan bon sang !

A. Annexe. Groupe symétrique : inversions, longueur, ordre de Bruhat

... like fabulous yellow roman candles exploding like spiders across the stars and in the middle you see the blue centerlight pop and everybody goes 'Awww!'

Jack Kerouac, *On the Road*, 1957

Cette annexe culmine avec l'*ordre de Bruhat* dans le groupe symétrique. C'est le pendant combinatoire de l'adhérence des cellules de Schubert dans les grassmanniennes, à l'instar de l'ordre de domination, des partitions (ou ordre de Chevalley) pour l'adhérence des orbites nilpotentes. Voilà notre motivation principale pour l'étudier.

Si la construction d'ensemble est complexe, on trouve sur la route quelques résultats élémentaires qui ont un intérêt indépendant : l'engendrement par les « transpositions simples » est classique et permet, par une étude rapide du nombre d'inversions, de montrer l'existence de la signature.

Soit n un entier non nul et soit $\mathfrak{S}_n$ le groupe symétrique sur n lettres.

A.1. Lemme (Engendrement par les transpositions simples). *Le groupe symétrique $\mathfrak{S}_n$, est engendré par les transpositions $s_i = (i, i+1)$ lorsque i parcourt $\{1, \ldots, n-1\}$.*

Voici une interprétation géométrique (ou plutôt topologique) du lemme.

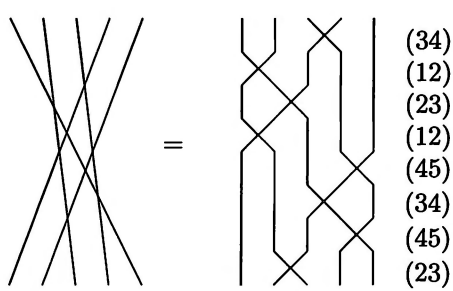


Figure A.1. $(15234) = (23)(45)(34)(45)(12)(23)(12)(34)$

Démonstration. On commence par montrer que les transpositions engendrent $\mathfrak{S}_n$. On procède par récurrence sur n. Pour $n = 1$, l'assertion est vide et pour $n = 2$, elle est triviale. Soit n un entier supérieur à 2, supposons que $\mathfrak{S}_{n-1}$ soit engendré par les transpositions. Soit w un élément de $\mathfrak{S}_n$. Si n est fixé par w, l'hypothèse de récurrence permet d'exprimer w comme produit de transpositions appartenant à $\mathfrak{S}_{n-1}$. Sinon, soient i l'image de n

par w et t la transposition (i,n). Alors tw fixe n donc c'est un produit de transpositions et w, que l'on peut écrire ttw, aussi. Cela conclut la récurrence.

Il suffit désormais de prouver que toute transposition est un produit des transpositions $s_i = (i,i+1)$ $(1 \leqslant i \leqslant n-1)$. Soient i et k entiers, avec $1 \leqslant i < i+k \leqslant n$. On peut exprimer la transposition $(i,i+k)$ ainsi :

$$(i,i+k) = s_i s_{i+1} \cdots s_{i+k-2} s_{i+k-1} s_{i+k-2} \cdots s_{i+1} s_i. \qquad \square$$

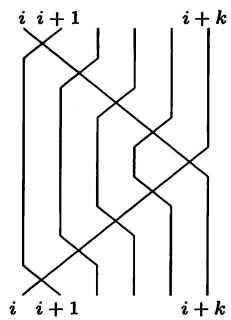


Figure A.2. *Transposition comme produit de transpositions élémentaires*

A.2. Notations. Rappelons que l'on a fixé n. On note S l'ensemble des transpositions $s_i = (i,i+1)$, où i décrit $\{1,\ldots,n-1\}$, et T l'ensemble des transpositions. Par principe de conjugaison, on a : $T = \bigcup_{w \in \mathfrak{S}_n} wSw^{-1}$.

Par ailleurs, on note Φ l'ensemble des couples (i,j) tels que $1 \leqslant i < j \leqslant n$. Attention à ne pas confondre le couple et la transposition correspondante.

A.3. Définition (Longueur d'une permutation). Soit w un élément du groupe $\mathfrak{S}_n$. On appelle *longueur* de w et l'on note $\ell(w)$ le nombre minimal de facteurs dans une expression de w comme produit de transpositions simples, c'est-à-dire le plus petit entier r pour lequel existent $s_{i_1},\ldots,s_{i_r} \in S$ tels que $w = s_{i_1} \cdots s_{i_r}$.

A.4. Exemples. La longueur de l'élément neutre est 0, la longueur d'un élément de S est 1.

Soit $w \in \mathfrak{S}_n$. Comme les éléments de S sont des involutions, l'égalité $w = s_{i_1} \cdots s_{i_r}$ donne : $w^{-1} = s_{i_r} \cdots s_{i_1}$. On en déduit l'inégalité $\ell(w^{-1}) \leqslant \ell(w)$ pour tout w, puis l'égalité : $\ell(w) = \ell(w^{-1})$ pour tout w.

Le premier jalon important de cette partie va consister à relier la longueur au nombre d'inversions.

A.5. Définition (Inversions d'une permutation). Soient n un entier et w un élément du groupe symétrique $\mathfrak{S}_n$. Une *inversion* de w est un couple d'entiers $(i,j) \in \Phi$ tel que $w(i) > w(j)$. On note

$$I(w) = \big\{(i,j) \in \{1,\dots,n\}^2 \,:\, i<j \text{ et } w(i)>w(j)\big\}$$

l'ensemble des inversions de w et $N(w)$ le *nombre d'inversions* de w.

A.6. Exemples. Soit w une transposition. Alors, $N(w)=0$ si et seulement si w est une application strictement croissante de $\{1,\dots,n\}$ dans lui-même, si et seulement si w est l'identité.

Soit $1 \leqslant i \leqslant n-1$, on a : $N(s_i) = 1$. Plus généralement, soit t une transposition, disons $t=(i,j)$ avec $i<j$, on a : $N(t) = (j-i)(j-i+1)/2$.

Posons $w_0(i) = n+1-i$ pour tout i, on a : $N(w_0) = n(n-1)/2$. On voit que w_0 est maximal pour le nombre d'inversions. On peut voir facilement en exercice qu'il s'agit de la seule permutation w telle que $N(w) = n(n-1)/2$.

A.7. Remarque. On sait que le groupe $\mathfrak{S}_n$ agit de façon doublement transitive sur $\{1,\dots,n\}$. Effectuons le changement de variables $i_0 = w(j)$, $j_0 = w(i)$. On a : $i<j$ et $w(i)>w(j)$ si et seulement si $i_0 < j_0$ et $w^{-1}(i_0) > w^{-1}(j_0)$, d'où l'on déduit : $N(w) = N(w^{-1})$.

À titre d'échauffement, on regarde l'effet du produit par une transposition simple sur les inversions.

A.8. Lemme. *Soient w un élément de $\mathfrak{S}_n$ et i compris entre 1 et $n-1$. Alors, on a*[16] :

$$I(ws_i) = s_i\big(I(w)\big)\triangle\big\{(i,i+1)\big\}.$$

Démonstration. Comme s_i fixe la paire $\{i,i+1\}$, s_i induit une bijection de $\Phi\setminus\{(i,i+1)\}$ sur lui-même. Cette bijection envoie $I(ws_i)\setminus\{(i,i+1)\}$ sur $I(w)\setminus\{(i,i+1)\}$: en effet, pour $(k,\ell)\in\Phi\setminus\{(i,i+1)\}$, on a :

$$(k,\ell)\in I(ws_i) \iff ws_i(k) > ws_i(\ell) \iff (s_i(k),s_i(\ell))\in I(w).$$

Par ailleurs, on a :

$$(i,i{+}1)\in I(w) \Leftrightarrow w(i)>w(i{+}1) \Leftrightarrow ws_i(i{+}1) > ws_i(i) \Leftrightarrow (i,i{+}1)\notin I(ws_i),$$

ce qui permet de conclure. □

[16] Ici, on note $\triangle$ la différence symétrique. Pour tout ensemble A, l'ensemble $A\triangle\{a\}$ est $A\cup\{a\}$ si $a\notin A$ et $A\setminus\{a\}$ si $a\in A$.

A.9. Proposition. *Soit w un élément du groupe $\mathfrak{S}_n$. Pour tout entier i compris entre 1 et $n-1$, on note s_i la transposition $(i, i+1)$. Alors :*

$$N(ws_i) = \begin{cases} N(w)+1 & \text{si } w(i) < w(i+1), \\ N(w)-1 & \text{si } w(i) > w(i+1)\,; \end{cases}$$

$$N(s_iw) = \begin{cases} N(w)+1 & \text{si } w^{-1}(i) < w^{-1}(i+1), \\ N(w)-1 & \text{si } w^{-1}(i) > w^{-1}(i+1). \end{cases}$$

Démonstration. La première égalité résulte directement du lemme A.8. Quant à la deuxième, on la déduit de la première et de la remarque A.7. □

On peut alors, si besoin est, montrer l'existence de la signature.

A.10. Corollaire. *L'application $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$, $w \mapsto (-1)^{N(w)}$ est un morphisme de groupes.*

Démonstration. Par la proposition A.9, on a : $\varepsilon(ws_i) = -\varepsilon(w)$ pour toute permutation w et tout entier i compris entre 1 et $n-1$.

Fixons une permutation w. Il existe des entiers $i_1, \ldots, i_\ell$ compris entre 1 et $n-1$ tels que $w = s_{i_1} \cdots s_{i_\ell}$. Une utilisation répétée de la formule précédente donne : $(-1)^\ell \varepsilon(w) = \varepsilon(ws_{i_\ell} \cdots s_{i_1}) = \varepsilon(\mathrm{Id}) = 1$.

Mais à présent, si w' est une nouvelle permutation, et $i'_1, \ldots, i'_{\ell'}$ des entiers tels que $w' = s_{i'_1} \cdots s_{i'_{\ell'}}$, on a par ce qui précède :

$$\varepsilon(ww') = \varepsilon(s_{i_1} \cdots s_{i_\ell} s_{i'_1} \cdots s_{i'_{\ell'}}) = (-1)^{\ell+\ell'} \varepsilon(\mathrm{Id}) = \varepsilon(w)\varepsilon(w'). \qquad \square$$

On peut à présent identifier longueur et nombre d'inversions.

A.11. Proposition. *Soit $w \in \mathfrak{S}_n$. On a : $N(w) = \ell(w)$.*

Démonstration. Soit $w = s_{i_1} \cdots s_{i_r}$ une décomposition de w comme produit de transpositions simples. Par la proposition A.9, multiplier à droite par une transposition simple ajoute au plus une inversion. En l'appliquant de façon répétée, on trouve donc : $N(w) \leqslant r$, d'où, si r est minimal : $N(w) \leqslant \ell(w)$.

Pour l'inégalité inverse, on montre par récurrence sur r que pour toute permutation w telle que $N(w) \leqslant r$, on a : $N(w) = \ell(w)$. L'initialisation est triviale : la seule permutation qui n'a pas d'inversion est l'identité, qui est de longueur nulle.

Supposons la propriété satisfaite pour un entier $r \geqslant 1$ et soit w une permutation ayant $r+1$ inversions. Il existe un entier i tel que $(i, i+1) \in I(w)$: sinon, w serait strictement croissante et ce serait l'identité. Il vient alors : $N(ws_i) = N(w) - 1$. Par hypothèse de récurrence, on peut décomposer ws_i sous la forme $ws_i = s_{i_1} \cdots s_{i_r}$, ce qui prouve que $\ell(w) \leqslant r+1$. Par la première partie de la preuve, il y a égalité et l'on peut conclure. □

Après ces préliminaires, on passe à l'*ordre de Bruhat.*

A.12. Définition. Soient $w, w' \in \mathfrak{S}_n$. On dit que w' est inférieur à w et l'on note $w' \leqslant w$ s'il existe une suite finie $w' = u_0, u_1, \dots, u_c = w$ de permutations et une suite $t_1, \dots, t_c$ de transpositions telles que $u_{i-1} = u_i t_i$ et $\ell(u_{i-1}) < \ell(u_i)$ pour tout $i \in \{1, \dots, c\}$. Si $c = 0$, la condition signifie que $w' = w$. Cette relation est manifestement réflexive ; antisymétrique puisque si $w \leqslant w'$, avec $w \neq w'$, alors $\ell(w') < \ell(w)$; et, par construction, transitive.

La relation $\leqslant$ s'appelle *l'ordre de Bruhat* sur le groupe symétrique.

A.13. Exercice. *Montrer que l'élément neutre e de $\mathfrak{S}_n$ est le plus petit élément pour l'ordre de Bruhat et que w_0 est l'élément le plus grand.*

Tel quel, l'ordre de Bruhat semble difficile à manipuler et sans rapport avec la décomposition en cellules de $\mathrm{GL}_n(\mathbb{K})$. Le but est de donner deux nouveaux critères pour remédier à cet état de fait. Pour commencer, nous aurons besoin d'une version plus générale de la proposition A.9.

A.14. Proposition. *Soient w un élément de $\mathfrak{S}_n$ et t une transposition, disons $t = (i, j)$ avec $i < j$. Alors, on a :*

$$N(wt) = \begin{cases} N(w) + 1 + 2|K| & \text{si } (i,j) \in I(w), \\ N(w) - 1 - 2|K| & \text{si } (i,j) \notin I(w), \end{cases}$$

où $K = K_{w,i,j}$ est l'ensemble des k strictement compris entre i et j tels que $w(k)$ soit compris entre $w(i)$ et $w(j)$.

Démonstration. Étant donnés k et ℓ avec $k < \ell$, on veut comparer les assertions « $(k, \ell) \in I(w)$ » et « $(k, \ell) \in I(wt)$ ».

- Si $k, \ell \notin \{i, j\}$, alors $(k, \ell) \in I(w) \Leftrightarrow (k, \ell) \in I(wt)$.
- Si $k < i$ et $\ell = i$, alors :
  $(k, i) \in I(w) \Leftrightarrow w(k) > w(i) \Leftrightarrow wt(k) < wt(j) \Leftrightarrow (k, j) \in I(wt)$.
  De même, on a : $(k, j) \in I(w) \Leftrightarrow (k, i) \in I(wt)$.
- Si $k = j$ et $\ell > j$, on a de même : $(i, \ell) \in I(w) \Leftrightarrow (j, \ell) \in I(wt)$ et $(j, \ell) \in I(w) \Leftrightarrow (i, \ell) \in I(wt)$.
- Si $k = i$ et $\ell = j$, alors $(i, j) \in I(w) \Leftrightarrow (i, j) \notin I(wt)$.
- Si $i < k < j$, de deux choses l'une :
  - ▷ si $w(k)$ n'est pas compris entre $w(i)$ et $w(j)$, alors $w(i) > w(k) \Leftrightarrow w(j) > w(k)$, si bien que l'on a : $(i, k) \in I(w) \Leftrightarrow (i, k) \notin I(wt)$ d'une part, et $(k, j) \in I(w) \Leftrightarrow (k, j) \notin I(wt)$ d'autre part ;
  - ▷ si $w(k)$ est compris entre $w(i)$ et $w(j)$, alors on a : $(i, k) \in I(w) \Leftrightarrow (i, k) \notin I(wt)$ et $(k, j) \in I(w) \Leftrightarrow (k, j) \notin I(wt)$.

Supposons que (i,j) soit une inversion de w. On voit que $N(wt)$ s'obtient de $N(w)$ en retranchant 1 pour le couple (i,j) et 2 pour chaque indice $k \in K$. Si (i,j) n'est pas une inversion de w, il suffit d'échanger les rôles de $w = wtt$ et wt. □

Il est temps de présenter la fameuse *condition d'échange*, valable dans le groupe symétrique, mais également dans tous les *groupes de Coxeter*, voir la remarque B.13.

A.15. Proposition (Condition d'échange). *Soit $w \in \mathfrak{S}_n$. Soit t une transposition telle que $\ell(wt) < \ell(w)$. Alors, pour toute décomposition réduite $w = s_{i_1} \cdots s_{i_r}$, il existe $k \in \{1, \ldots, r\}$ tel que $wt = s_{i_1} \cdots \widehat{s_{i_k}} \cdots s_{i_r}$, où le chapeau sur s_{i_k} signifie que ce facteur est omis.*

Démonstration. Notons $t = (i,j)$ avec $i < j$. Par la proposition A.14, l'inégalité $\ell(wt) < \ell(w)$ entraîne que (i,j) appartient à $I(w)$. Ainsi, pour $k = 1$, on a : $s_{i_k} \cdots s_{i_r}(i) > s_{i_k} \cdots s_{i_r}(j)$. En le choisissant maximal, on peut donc trouver un indice k compris entre 1 et r tel que :

$$s_{i_k} \cdots s_{i_r}(i) > s_{i_k} \cdots s_{i_r}(j) \quad \text{et} \quad s_{i_{k+1}} \cdots s_{i_r}(i) < s_{i_{k+1}} \cdots s_{i_r}(j).$$

Pour un tel indice k, le couple $\big(s_{i_{k+1}} \cdots s_{i_r}(i), s_{i_{k+1}} \cdots s_{i_r}(j)\big)$ est une inversion de s_{i_k} : il est donc égal au couple $(i_k, i_k + 1)$. Par principe de conjugaison, les transpositions correspondantes sont reliées par l'égalité

$$s_{i_k} = s_{i_{k+1}} \cdots s_{i_r}\, t\, (s_{i_{k+1}} \cdots s_{i_r})^{-1},$$

ce qui donne, en multipliant par $s_{i_{k+1}} \cdots s_{i_r} t$:

$$s_{i_k}\, s_{i_{k+1}} \cdots s_{i_r}\, t = s_{i_{k+1}} \cdots s_{i_r},$$

puis, en multipliant par $s_{i_1} \cdots s_{i_{k-1}}$:

$$wt = s_{i_1} \cdots \widehat{s_{i_k}} \cdots s_{i_r}.$$ □

A.16. Définition (Sous-expression). Soit w un élément de $\mathfrak{S}_n$. Si $w = s_{i_1} \cdots s_{i_r}$ est une expression de w comme produit d'éléments de S, une *sous-expression* de w est un élément de la forme $w' = s_{i_{\varphi(1)}} \cdots s_{i_{\varphi(q)}}$, où $1 \leqslant q \leqslant r$ et $\varphi(1) < \cdots < \varphi(q)$. Si l'expression initiale est réduite, on dit que w' est obtenu de w *par décimation*.

A.17. Proposition (Ordre de Bruhat par décimation). *Soient w et w' deux éléments de $\mathfrak{S}_n$. Alors, $w' \leqslant w$ si et seulement si w' est obtenu de w par décimation.*

Démonstration. Supposons que $w' \leqslant w$. Par construction de l'ordre de Bruhat, cela implique que w' est obtenu par décimation à partir de w par une application répétée de la condition d'échange A.15.

Pour la réciproque, on suppose d'abord que $w = s_{i_1} \cdots s_{i_r}$, avec $r = \ell(w)$, et que $w' = s_{i_1} \cdots \widehat{s_{i_k}} \cdots s_{i_r}$ pour $1 \leqslant k \leqslant r$ convenable. Posons alors $t = x s_{i_k} x^{-1}$, où $x = s_{i_r} \cdots s_{i_{k+1}}$, de sorte que l'on a : $wt = w'$. De plus, comme r est la longueur de w et que w' admet une expression avec $r-1$ générateurs, on a clairement : $\ell(w') < \ell(w)$. Il vient donc : $w' \leqslant w$. Si w' est obtenu par décimation à partir de w, il suffit d'appliquer plusieurs fois cette propriété. □

Cette caractérisation a une conséquence amusante.

A.18. Corollaire. *Dans le groupe symétrique, l'application de passage à l'inverse est strictement croissante pour l'ordre de Bruhat.*

Démonstration. Il suffit de remarquer que si $w = s_{i_1} \cdots s_{i_r}$, alors $w^{-1} = s_{i_r} \cdots s_{i_1}$, si bien que w' est obtenu de w par décimation si et seulement si w'^{-1} est obtenu de w^{-1} par décimation. □

On peut alors échanger la droite et la gauche dans l'ordre de Bruhat.

A.19. Corollaire

(i) *Soient $w \in \mathfrak{S}_n$ et t une transposition, disons $t = (i,j)$ avec $i < j$. Alors : $tw \leqslant w$ si et seulement si $w^{-1}(i) > w^{-1}(j)$, c'est-à-dire que (i,j) est une inversion de w^{-1}.*

(ii) *Soient w et w' deux transpositions. Alors $w' \leqslant w$ si et seulement s'il existe une suite finie $w' = w_0 < w_1 < \cdots < w_c = w$ et des transpositions $t_1, \ldots, t_c$ telles que $w_{i-1} = t_i w_i$ pour tout i.*

Démonstration. (i) Par le corollaire A.18, la condition $tw \leqslant w$ équivaut à la condition $w^{-1}t \leqslant w^{-1}$, que l'on sait, par la proposition A.14, équivalente au fait que (i,j) est une inversion de w^{-1}.

(ii) Toujours par le corollaire A.18, $w' \leqslant w$ équivaut à $w'^{-1} \leqslant w^{-1}$, donc à l'existence d'une suite de permutations $w'^{-1} = x_0 < x_1 < \cdots < x_c = w^{-1}$ et de transpositions $t_1, \ldots, t_c$ telles que $x_{i-1} = x_i t_i$ pour tout i. Il suffit de poser $w_i = x_i^{-1}$, étant donné qu'alors, $x_{i-1} < x_i$ équivaut à $w_{i-1} < w_i$ pour tout i. □

À présent, on veut identifier l'ordre de Bruhat que l'on vient de le définir et l'*ordre d'Ehresmann*, qui apparaît dans le paragraphe 3.16.

A.20. Définition. Soit $w \in \mathfrak{S}_n$. Pour $1 \leqslant j \leqslant k \leqslant n$, on note $w[k,j]$ le j-ème élément (pour l'ordre naturel de $\mathbb{N}$) de $\{w(1), \ldots, w(k)\}$. On définit le *tableau* associé à w comme la famille d'entiers $T(w) = (w[k,j])_{1 \leqslant j \leqslant k \leqslant n}$.

Ainsi, pour $k \in \{1, \dots, n\}$, on a :
- d'une part, $\{w[k,1], w[k,2], \dots, w[k,k]\} = \{w(1), w(2), \dots, w(k)\}$;
- d'autre part, $1 \leqslant w[k,1] < w[k,2] < \cdots < w[k,k] \leqslant n$.

A.21. Exemples. Prenons $n = 4$, observons quelques tableaux :
- pour $w = (1423) = s_2 s_3 s_2 s_1 s_2$, on a : $T(w) = \begin{smallmatrix} & & & 4 \\ & & 3 & 4 \\ & 1 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{smallmatrix}$;
- pour $v = (1342) = s_2 s_3 s_1$, on a : $T(v) = \begin{smallmatrix} & & 3 & \\ & 1 & 3 & \\ 1 & 3 & 4 & \\ 1 & 2 & 3 & 4 \end{smallmatrix}$;
- pour $u = (24) = s_2 s_3 s_2$, on a : $T(u) = \begin{smallmatrix} & & 1 & \\ & 1 & 4 & \\ 1 & 3 & 4 & \\ 1 & 2 & 3 & 4 \end{smallmatrix}$.

A.22. Remarque. L'application $w \mapsto T(w)$ est injective puisque l'image d'un entier k s'écrit :

$$\{w(k)\} = \{w[k,j],\ 1 \leqslant j \leqslant k\} \setminus \{w[k-1,j],\ 1 \leqslant j < k\}.$$

A.23. Définition. On définit l'ordre d'Ehresmann sur $\mathfrak{S}_n$ ainsi. Pour $w, w' \in \mathfrak{S}_n$, on note $T(w) = (w[k,j])_{1 \leqslant j \leqslant k \leqslant n}$ et $T(w') = (w'[k,j])_{1 \leqslant j \leqslant k \leqslant n}$ les tableaux associés. On dit que w est inférieur ou égal à w' si, pour tout $1 \leqslant j \leqslant k \leqslant n$, on a : $w[k,j] \leqslant w'[k,j]$. (En termes des *types* rencontrés au tome premier, cela signifie que pour tout k, le type $\{w(1), \dots, w(k)\}$ est inférieur ou égal à $\{w'(1), \dots, w'(k)\}$.)

A.24. Exemples. Aussi bien pour l'ordre de Bruhat (par décimation) que pour l'ordre d'Ehresmann, on a alors dans les exemples A.21 : $v \leqslant w$ et $u \leqslant w$, que u et v ne sont pas comparables.

A.25. Proposition. *Les ordres de Bruhat et d'Ehresmann coïncident.*

On commence par deux lemmes plus faciles à voir qu'à formaliser.

A.26. Lemme. *Si $w \in \mathfrak{S}_n$ et $1 \leqslant j \leqslant k < n$, alors $w[k+1,j] \leqslant w[k,j]$.*

Démonstration (du lemme). La $(k+1)$-ième ligne de $T(w)$ s'obtient en insérant $w(k+1)$ dans la liste $w[k,1] < \cdots < w[k,k]$. Soit r l'indice tel que $w[k+1,r] = w(k+1)$. On a donc : $w[k,r-1] < w(k+1) < w[k,r]$. Ainsi, si $j < r$, alors $w[k+1,j] = w[k,j]$; si $j = r$, alors $w[k+1,r] = w(k+1) < w[k,r]$; si $j > r$, alors $w[k+1,j] = w[k,j-1] < w[k,j]$. □

A.27. Lemme. *Soient w et w' deux permutations et k compris entre 1 et $n-1$. On suppose que si $1 \leqslant j \leqslant k$, alors $w'[k,j] = w[k,j]$, et que $w'(k+1) \leqslant w(k+1)$. Alors, si $1 \leqslant j \leqslant k+1$, on a : $w'[k+1,j] \leqslant w[k+1,j]$.*

Démonstration (du lemme). Soit r (resp. r') l'indice tel que $w[k+1,r] = w(k+1)$ (resp. $w'[k+1,r'] = w'(k+1)$). Comme $w'(k+1) \leqslant w(k+1)$, on a : $r' \leqslant r$. Pour $j < r'$, $w'[k+1,j] = w[k+1,j]$. On a : $w'[k+1,r'] < w'[k+1,r'+1] = w'[k,r'] \leqslant w[k,r'] = w[k+1,r']$. Pour $r' < j < r$, $w'[k+1,j] = w'[k,j-1] \leqslant w[k,j-1] \leqslant w[k,j] = w[k+1,j]$. On a : $w'[k+1,r] \leqslant w[k,r-1] < w(k+1) = w[k+1,r]$. Enfin, si $r < j$, $w'[k+1,j] = w'[k,j-1] \leqslant w[k,j-1] = w[k+1,j]$. □

Démonstration (de la proposition). Soient w et w' deux permutations de $\mathfrak{S}_n$. Supposons que $w' \leqslant w$ et montrons que $T(w') \leqslant T(w)$. Par le corollaire A.19 et par transitivité de l'ordre d'Ehresmann, on peut supposer que $w' = tw$, où t est une transposition, disons $t = (i,j)$ avec $i < j$ et $a = w^{-1}(i) > w^{-1}(j) = b$. On représente w et tw par les images de 1, 2, etc. :

$$w = [w(1), \ldots, w(b-1), j, w(b+1), \ldots, w(a-1), i, w(a+1), \ldots, w(n)],$$

$$tw = [w(1), \ldots, w(b-1), i, w(b+1), \ldots, w(a-1), j, w(a+1), \ldots, w(n)],$$

Pour $k < b$ ou $k \geqslant a$, les ensembles $\{w(1), \ldots, w(k)\}$ et $\{tw(1), \ldots, tw(k)\}$ coïncident, d'où : $tw[k,\ell] \leqslant w[k,\ell]$ pour $1 \leqslant \ell \leqslant k$. Pour $b \leqslant k < a$, on utilise le lemme A.27.

Réciproquement, supposons que $T(w') < T(w)$. Soit k_0 l'entier minimal tel que $w'(k) \neq w(k)$. Par minimalité, $w'(k_0)$ n'est pas l'image par w d'un élément de $\{1, \ldots, k_0\}$, si bien qu'il existe k_1 tel que $w'(k_0) \leqslant w(k_1) < w(k_0)$. On choisit k_1 minimal. Enfin, on note t la transposition $t = (w(k_1), w(k_0))$.

Par construction, $w(k_1) < w(k_0)$ et $k_1 > k_0$, donc $tw < w$. On va montrer que $T(w') \leqslant T(tw)$. Le tableau $T(tw)$ s'obtient de $T(w)$ en remplaçant $w(k_0)$ par $w(k_1)$ dans les lignes k_0 à $k_1 - 1$ et en réordonnant ces lignes. (En effet, si $k < k_0$, ni $w(k_0)$ ni $w(k_1)$ n'apparaissent dans $\{w(1), \ldots, w(k)\}$; si $k > k_1$, tous deux y apparaissent.) Comme par hypothèse, $T(w') \leqslant T(w)$, on a : $w'[k,j] \leqslant tw[k,j]$ pour tout k tel que $k < k_0$ ou $k \geqslant k_1$ et tout $1 \leqslant j \leqslant k$.

Soit $k_0 \leqslant k < k_1$. Soit r le rang de $w(k_0)$ dans $\{w(1), \ldots, w(k)\}$, *i.e.* : $w[k,r] = w(k_0)$. C'est aussi le rang auquel $tw(k_0) = w(k_1)$ apparaît dans $\{tw(1), \ldots, tw(k)\}$, *i.e.* : $tw[k,r] = tw(k_0)$. Sinon, il y aurait un indice $k_2 < k_1$ tel que $w(k_1) < w(k_2) < w(k_0)$, ce qui contredirait la minimalité de k_1.

On montre par récurrence finie sur $k \geqslant k_0$ que pour tout j compris entre 1 et k, on a : $w'[k,j] \leqslant tw[k,j]$. Pour $j \neq r$, il n'y a rien à démontrer puisque $tw[k,j] = w[k,j]$.

Observons la ligne k_0. Par définition de k_0, on a : $w'(j) = w(j) = tw(j)$ si $1 \leqslant j < k_0$ et $w'(k_0) \leqslant tw(k_0)$. On peut donc lui appliquer le lemme A.27 et il vient : $w'[k_0,r] \leqslant tw[k_0,r]$.

Supposons la propriété vraie pour $k \geqslant k_0$ (avec $k < k_1 - 1$, sinon on connaît déjà le résultat). Soient r tel que $tw[k,r] = tw(k_0)$, et s tel que $tw[k+1,s] = tw(k_0)$. On distingue deux cas.

Premier cas : Si $w(k+1) < w'(k_0) \leqslant tw(k_0)$, alors $tw(k_0) = tw[k+1, r+1]$ (*i.e.* $s = r+1$). Comme $w'[k+1, r] < w'(k_0)$ et que $w'[k+1, r+1]$ est le suivant dans la liste, on a : $w'[k+1, r+1] \leqslant w'(k_0) \leqslant tw(k_0) = tw[k+1, r+1]$.

Deuxième cas : Si $w(k+1) \geqslant w'(k_0)$, alors $w(k+1) \geqslant w(k_1)$ (par définition de k_1) et $tw(k_0) = tw[k+1, r]$ (*i.e.* $s = r$). Il vient avec le lemme A.26 : $w'[k+1, r] \leqslant w'[k, r] \leqslant tw(k_0) = tw[k+1, r]$.

On a bien montré que $T(w') \leqslant T(tw)$. Par récurrence sur la longueur d'une chaîne[17], on en déduit alors que $w' \leqslant tw$, puis l'on conclut que $w' < w$. □

A.28. Exemples. Voici les *posets* de l'ordre de Bruhat de $\mathfrak{S}_2$, $\mathfrak{S}_3$ et $\mathfrak{S}_4$ ainsi que les préordres $\preceq_m$. Le symbole $[w_1 \cdots w_n]$ désigne la permutation $i \mapsto w_i$ $(1 \leqslant i \leqslant n)$.

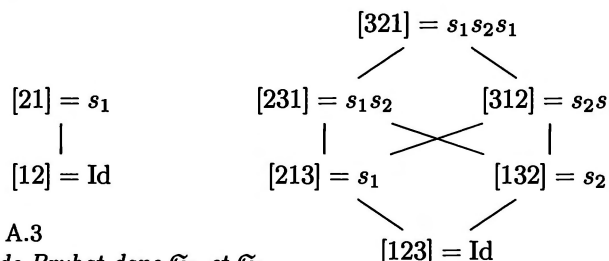


Figure A.3
Ordre de Bruhat dans $\mathfrak{S}_2$ *et* $\mathfrak{S}_3$

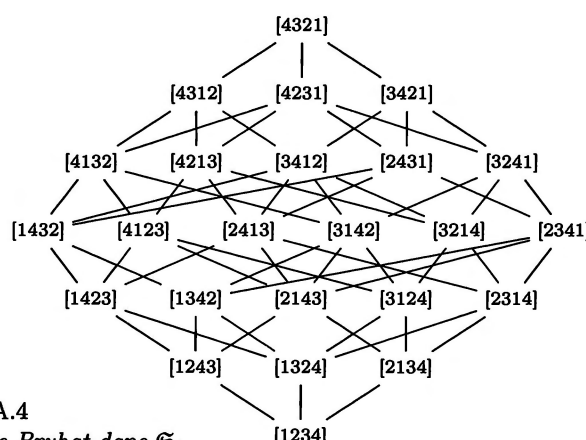


Figure A.4
Ordre de Bruhat dans $\mathfrak{S}_4$

Gnignigni... C'est de la bouillie, tout ça !

[17] Dans un ensemble partiellement ordonné (*poset*), une chaîne est une suite finie totalement ordonnée. Ici, la longueur maximale d'une chaîne de w' à tw est strictement plus petite que celle d'une chaîne de w' à w.

B. Addendum. Présentation du groupe symétrique *et al.*

Dans ce paragraphe, on raffine considérablement le lemme A.1 en donnant une *présentation* du groupe symétrique. On en tire une construction (de plus) de la signature et une application originale aux automorphismes extérieurs de $\mathfrak{S}_6$, voir les exercices C.22 et V-D.11 .

B.1. Généralités

La notion de groupe libre et de présentation de groupe est expliquée par exemple dans les livres [56] et [14]. Expliquons tout de même brièvement de quoi il s'agit.

Soit n un entier positif. Il existe un groupe libre L_n à n générateurs, unique à isomorphisme près. Par construction (on l'omettra), le groupe L_n, d'élément neutre e, est muni d'une famille de générateurs $(\ell_k)_{1\leqslant k\leqslant n}$ qui est une *famille libre*, au sens où, si

$$\ell_{k_1}^{a_1}\cdots\ell_{k_m}^{a_m}=e,$$

avec $k_i\neq k_{i+1}$ et $a_i\in\mathbb{Z}\setminus\{0\}$ pour tout $i\in\{1,\dots,m\}$, alors m est nul[18].

Le groupe L_n possède la *propriété universelle* suivante : pour tout groupe G et toute famille $(x_k)_{1\leqslant k\leqslant n}$ d'éléments de G, il existe un unique morphisme de L_n vers G qui envoie ℓ_k sur x_k pour tout k.[19]

Maintenant, supposons que G soit engendré par le système $(g_k)_{1\leqslant k\leqslant n}$. Alors, le morphisme φ qui envoie ℓ_k sur g_k pour tout k est surjectif, de sorte que le groupe G est isomorphe à $L_n/\ker\varphi$.

Ajoutons aux données une famille (finie ou pas) $(r_i)_{i\in I}$ d'éléments de $\ker\varphi$ telle que $\ker\varphi$ est le plus petit sous-groupe distingué contenant les r_i. Autrement dit, $\ker\varphi$ est le sous-groupe engendré par les gr_ig^{-1}, où g parcourt L_n et i parcourt I. Concrètement, cela signifie que dans le quotient[20] $L_n/\ker\varphi$, on a : $\bar{x}\bar{r}_i\bar{y}=\bar{x}\bar{y}$ pour tout i et tous x, y de L_n et que $L_n/\ker\varphi$ est le plus grand groupe quotient de L_n dans lequel cette relation est vraie. Les éléments r_i sont appelés relations, et $(r_i)_{i\in I}$ est un *système de relations*. On dit aussi que $r_i=1$ $(i\in I)$, ou toute autre (famille d')égalité(s) équivalente(s), est un système de relations.

---

[18] On voit bien comment, partant d'une expression où ces conditions ne seraient pas remplies, la réduire en une expression plus courte en remplaçant $\ell_{k_i}^{a_i}\ell_{k_{i+1}}^{a_{i+1}}$ par $\ell_{k_i}^{a_i+a_{i+1}}$ si $k_i=k_{i+1}$ ou en omettant $\ell_{k_i}^{a_i}$ si $a_i=0$, et en recommençant autant de fois que nécessaire. La propriété de liberté exprime que ces ambiguïtés d'écriture triviales sont les seules.

[19] C'est cette propriété qui assure l'unicité au sens fort : si L'_n est un autre groupe libre engendré par $(\ell'_k)_{1\leqslant k\leqslant n}$, il existe un unique isomorphisme $\varphi : L_n\to L'_n$ qui envoie ℓ_k sur ℓ'_k pour tout k.

[20] On note $g\mapsto\bar{g}$ le passage au quotient.

La double donnée d'une famille de générateurs $(g_k)_{1\leqslant k\leqslant n}$ et d'un système de relations $(r_i)_{i\in I}$ est appelée *présentation de G par générateurs et relations*. Elle peut être très utile puisqu'elle permet de construire facilement les morphismes de G dans un groupe quelconque G'. En effet, pour toute famille $(g'_k)_{1\leqslant k\leqslant n}$ d'éléments de G' qui satisfont[21] aux relations r_i $(i\in I)$, il existe un unique morphisme $\bar{\varphi} : G \to G'$ qui envoie g_k sur g'_k pour tout k.

En décalant un peu le point de vue, on peut se donner simplement un entier n et une famille d'éléments $R = (r_i)_{i\in I}$ du groupe libre L_n et se demander s'il existe un groupe G et une famille de générateurs $(g_k)_{1\leqslant k\leqslant n}$ pour lesquels (g_k) et (r_i) soient une présentation. La réponse est oui et la construction est presque évidente : on définit K comme le plus petit sous-groupe distingué engendré par les r_i $(i\in I)$, c'est-à-dire le sous-groupe de L_n engendré par les gr_ig^{-1} $(i\in I,\ g\in G)$, on prend pour G le quotient L_n/K et pour g_k l'image de ℓ_k dans G. Ce groupe est solution d'un problème universel décrit informellement dans le paragraphe précédent et plus précisément dans les références [56] et [14].

Dans ce contexte, la notation consacrée pour G est : $G = \langle \ell_1, \ldots, \ell_n | R\rangle$. Il va de soi que l'on peut *ad libitum* remplacer les noms $\ell_1, \ldots, \ell_n$ par d'autres symboles.

B.2. Exemple. Le groupe libre L_0 est le groupe trivial à 1 élément. Le groupe libre L_1 à 1 générateur est $\mathbb{Z}$. On retrouvera le groupe L_2 au §VII-3 (proposition VII-3.2 et figure VII-3.3).

B.3. Exemple. Si la famille R est vide, le groupe présenté par n générateurs et pas de relation est le groupe libre L_n.

B.4. Exemple. Le groupe $G = \mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par $\bar{1}$. On a donc un morphisme $\varphi : L_1 = \mathbb{Z} \to Z/n\mathbb{Z}$, déterminé par $1 \mapsto \bar{1}$, tel que $\ker\varphi = n\mathbb{Z}$ engendré par n. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est donc présenté par le générateur $\bar{1}$ et la relation n (qui engendre $n\mathbb{Z}$). On voit donc que pour construire un morphisme φ de G dans un groupe G', il suffit de se donner une image de $\bar{1}$ telle que $n\varphi(\bar{1}) = 0$. La propriété d'universalité citée plus haut et le passage au quotient assurent l'existence du morphisme φ.

B.5. Exemple. Le *groupe diédral* D_n ne serait plus à présenter. Eh bien si, justement, on va le faire ! On le définit comme le groupe des isométries « du » polygone régulier à n sommets du plan. Il contient les n rotations du polygone et ses n réflexions par rapport aux n axes de symétrie du polygone. Si s est une réflexion et r une rotation d'ordre n, on voit que

[21] Sens : pour tout i, l'élément r_i s'écrit de façon unique $r_i = \ell_{k_1}^{a_1}\cdots\ell_{k_m}^{a_m}$, avec les contraintes énoncées plus haut ; on demande que $(g'_{k_1})^{a_1}\ldots(g'_{k_m})^{a_m}$ soit le neutre de G'.

$D_n = \{e, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$. Le groupe D_n est donc engendré par les r et s et l'on a : $r^n = s^2 = (sr)^2 = e$. On peut donc, par la propriété universelle, construire un morphisme surjectif φ de L_2, engendré par $\ell_1 = R$ et $\ell_2 = S$, tel que $R \mapsto r$ et $S \mapsto s$. Son noyau $\ker\varphi$ contient donc R^n, S^2 et $(SR)^2$.

On veut montrer que l'on a là une présentation de D_n. Soit K' le plus petit sous-groupe distingué contenant ces relations, alors $K' \subset \ker\varphi$. Pour montrer l'égalité, il suffit de voir que $|L_2/K'| = |L_2/\ker\varphi|$, c'est-à-dire que $|L_2/K'| = |D_n| = 2n$. On a bien sûr l'inégalité $|L_2/K'| \geqslant 2n$, puisque l'on a établi une surjection de L_2, et donc par passage au quotient, de L_2/K', sur D_n. Reste à montrer l'inégalité inverse. On peut remarquer que dans L_2/K', on a : $\bar{S}\bar{R} = \bar{R}^{-1}\bar{S}$. Par récurrence, tout produit $\bar{S}^k\bar{R}^\ell$ peut s'écrire sous la forme $\bar{R}^{\ell'}\bar{S}^{k'}$. Une autre récurrence montre alors que tout élément de L_2/K' peut s'écrire $\bar{R}^{\ell'}\bar{S}^{k'}$, avec $\ell', k' \in \mathbb{Z}$. Comme $R^n = S^2 = 1$, on peut choisir ℓ' dans $\{0, \dots, n-1\}$ et $k' \in \{0, 1\}$. Cela donne la propriété voulue.

On a donc : $D_n \simeq \langle r, s \,|\, r^n, s^2, (rs)^2\rangle$.

B.6. Exercice. *Soit n un entier non nul.*

1. *Montrer que le produit semi-direct $D'_n = \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ défini par l'action : $\varphi_{\bar{1}}(\bar{x}) = -\bar{x}$ $(x \in \mathbb{Z}/n\mathbb{Z})$ admet la même présentation que D_n.*
   Évidemment, il ne s'agit pas d'utiliser l'isomorphisme connu entre D_n et D'_n. On vérifiera que ce groupe est engendré par un générateur de $\mathbb{Z}/n\mathbb{Z}$ et un de $\mathbb{Z}/2\mathbb{Z}$, on exhibera un morphisme de $\langle r, s | r^n, s^2, (rs)^2\rangle$ vers D'_n et l'on montrera qu'il est bijectif.
2. *Montrer que l'on a la présentation suivante : $D_n \simeq \langle s, t | s^2, t^2, (st)^n\rangle$.*
   Prendre $t = sr$ dans la présentation précédente.
3. *En utilisant cette présentation, montrer qu'il existe 2 ou 4 morphismes $\varepsilon : D_n \to \mathbb{C}^*$ selon la parité de n.*
   Vérifier que $\varepsilon(s)$ et $\varepsilon(t)$ valent ± 1. Montrer grâce à la présentation que s et t sont conjugués si n est impair et grâce à la géométrie qu'ils ne le sont pas si n est pair.

Voici la présentation la plus classique de $\mathfrak{S}_n$.

B.7. Proposition. *Pour $n \geqslant 2$, le groupe symétrique $\mathfrak{S}_n$ est présenté par générateurs $s_1, \dots, s_{n-1}$ et relations « de Coxeter » :*

$$\begin{cases} \forall i = 1, \dots, n-1, & s_i^2 = 1 \\ \forall i = 1, \dots, n-1, & s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, \\ \forall i, j = 1, \dots, n-1,\ |i-j| \geqslant 2, & s_i s_j = s_j s_i. \end{cases}$$

B.8. Remarque. On vérifie sans peine que les éléments $(i, i+1)$ de $\mathfrak{S}_n$ satisfont aux relations de G_n — par exemple graphiquement.

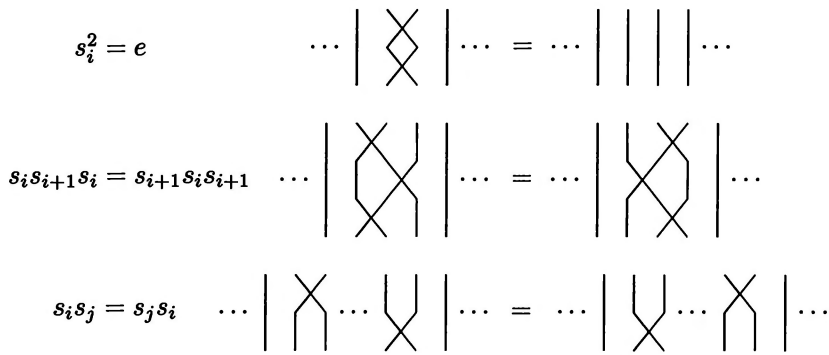


Figure B.1. *Relations de Coxeter dans* $\mathfrak{S}_n$

Cela prouve seulement que $\mathfrak{S}_n$ est un quotient du groupe présenté dans la proposition. Comme pour le groupe diédral, on majore le cardinal de notre groupe en utilisant une « forme normale ». Voici la clé.

B.9. Lemme. *Soit G_n le groupe admettant la présentation de la proposition B.7. Tout élément $w \in G_n$ peut s'écrire sous la forme :*

$$w = \underbrace{s_{i_{n-1}} s_{i_{n-1}+1} \cdots s_{n-1}}\ \underbrace{s_{i_{n-2}} s_{i_{n-2}+1} \cdots s_{n-2}}\ \cdots\ \underbrace{s_{i_k} s_{i_k+1} \cdots s_{k-1} s_k}\ \cdots$$

où $1 \leqslant i_k \leqslant k+1$ pour $k = 1, \ldots, n-1$, avec la convention que si $i_k = k+1$, on n'écrit pas le « paquet » correspondant.

Le lemme signifie que tout élément s'obtient en supprimant les premières lettres de chaque paquet à partir de la décomposition suivante de l'élément le plus long :

$$w_0 = \underbrace{s_1 s_2 \cdots s_{n-2} s_{n-1}}\ \underbrace{s_1 s_2 \cdots s_{n-3} s_{n-2}}\ \cdots\ \underbrace{s_1 s_2 s_3}\ \underbrace{s_1 s_2}\ \underbrace{s_1}\ .$$

Démonstration (du lemme). On procède par récurrence sur n — c'est trivial pour $n \leqslant 2$. On suppose l'assertion vraie pour le groupe G_n engendré par $s_1, \ldots, s_{n-1}$, et l'on la prouve pour G_{n+1}.

Premier pas. Tout élément $w \in G_{n+1}$ peut s'écrire avec au plus une occurrence de s_n. En effet, considérons une écriture de w comme produit des s_i $(i = 1, \ldots, n)$ contenant un nombre minimal d'occurrences de s_n, et supposons qu'il y en ait au moins deux. Il existe donc w' dans le groupe engendré

par $s_1, \dots, s_{n-1}$ et $x, y \in G_{n+1}$ tels que

$$w = x\, s_n\, w'\, s_n\, y.$$

Par hypothèse de récurrence, il y a deux cas : w' s'écrit sous la forme $s_i s_{i+1} \cdots s_{n-1} w''$, avec $i \leqslant n-1$, ou alors $w' = w''$, où, dans les deux cas, w'' est un produit des éléments $s_1, \dots, s_{n-2}$: w'' commute avec s_n. Dans le premier cas, on a :

$$\begin{aligned} w &= x s_n s_i s_{i+1} \cdots s_{n-1} w'' s_n y = x s_i s_{i+1} \cdots s_{n-2} s_n s_{n-1} s_n w'' y \\ &= x s_i s_{i+1} \cdots s_{n-2} s_{n-1} s_n s_{n-1} w'' y. \end{aligned}$$

Dans le deuxième cas :

$$w = x s_n w'' s_n y = x w'' s_n^2 y = x w'' y.$$

Dans les deux cas, l'écriture obtenue contredit la minimalité du nombre d'occurrences de s_n dans l'écriture initiale, ce qui prouve le premier pas.

Deuxième pas. On achève le lemme. Soit $w \in G_n$. Si w peut s'écrire sans s_n, l'hypothèse de récurrence s'applique et donne une écriture de w qui convient. Sinon, d'après le premier pas, w peut s'écrire sous la forme

$$w = x s_n y,$$

où x et y sont des produits de $s_1, \dots, s_{n-1}$. Par hypothèse de récurrence, notre x s'écrit $s_i s_{i+1} \cdots s_{n-1} z$ ou $x = z$, où z est un produit de $s_1, \dots, s_{n-2}$, c'est-à-dire z commute avec s_n. Dans le premier cas, on a :

$$x = s_i s_{i+1} \cdots s_{n-1} s_n\, zy,$$

et dans le deuxième cas :

$$x = zy.$$

Dans chaque cas, l'hypothèse de récurrence appliquée à zy permet de conclure. □

Démonstration (de la proposition). D'après le lemme, le cardinal du groupe G_n est au plus $n \times (n-1) \times \cdots \times 2 = n!$. Or, dans la remarque B.8, on a mis en évidence une surjection $G_n \to \mathfrak{S}_n$ et le cardinal de $\mathfrak{S}_n$ est $n!$. Il en résulte que notre surjection est un isomorphisme, et, de plus, que l'écriture dans le lemme est *unique.* □

B.10. Remarque. Voir l'exercice C.27 pour une présentation alternative, et aussi pour une méthode alternative qui peut parfaitement s'adapter à une preuve de cette proposition.

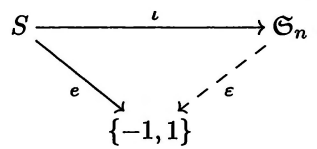
Cette présentation donne une construction de plus de la signature...

B.11. Corollaire. *Il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ non trivial : la signature, qui envoie chaque générateur s_i sur -1.*

Démonstration. On utilise la propriété universelle d'une présentation. On caractérise un morphisme par l'image des s_i, qui engendrent $\mathfrak{S}_n$, c'est-à-dire par une application $e : S \to \mathbb{C}^*$, où $S = \{s_1, \dots, s_{n-1}\}$. Le système

$$\begin{cases} e(s_i)^2 = 1, & \text{si } i \leqslant n-1, \\ e(s_i)e(s_{i+1})e(s_i) = e(s_{i+1})e(s_i)e(s_{i+1}) & \text{si } i \leqslant n-2, \\ e(s_i)e(s_j) = 1 = e(s_j)e(s_i) & \text{si } |i-j| \geqslant 2 \end{cases}$$

est une condition nécessaire et suffisante pour qu'il existe un morphisme de groupe ε qui prolonge e, c'est-à-dire qui fait commuter le diagramme :



Résolvons ce système. On a nécessairement : $e(s_i) \in \{-1, 1\}$ pour tout i. D'après la deuxième série de relations, pour $i \leqslant n-2$, on a : $e(s_i) = e(s_{i+1})$. Ainsi, e est nécessairement constante.

Si $e(s_i) = 1$ pour tout i, le système est satisfait et le morphisme ε est trivial ; si $e(s_i) = -1$, le système est encore satisfait et l'on retrouve la signature. □

B.12. Remarque. Dans la preuve précédente, on a simplifié $e(s_i)e(s_{i+1})$, ce qui cache que s_i et s_{i+1} sont conjugués. En effet : $(s_i s_{i+1})s_i(s_i s_{i+1})^{-1} = s_{i+1}$ car $(s_i s_{i+1})^3 = e$ et $s_i^2 = e = s_{i+1}^2$.

B.13. Remarque. Le groupe symétrique $\mathfrak{S}_n$ est la figure de proue des *groupes de Coxeter* sur lesquels beaucoup d'encre a coulé et coule encore. Par définition, un groupe de Coxeter admet une présentation de la forme $\langle r_1, r_2 \dots, r_n | (r_i r_j)^{m_{ij}} \rangle$, où $m_{ij} \in \mathbb{N} \cup \{\infty\}$, $m_{ii} = 1$ pour tout i (les r_i sont des involutions), $m_{ij} = m_{ji} \geqslant 2$ pour $i \neq j$. Les r_i sont appelées *réflexions*, vocable justifié par l'existence d'une réalisation d'un groupe de Coxeter dans le groupe orthogonal d'un espace réel — euclidien si le groupe est fini — dans laquelle les s_i fixent un hyperplan. La référence standard sur le sujet est [10].

L'exercice B.6 montre que D_n est également un groupe de Coxeter.

C'était pas mauvais, c'était très *mauvais.*
Gérard Oury, *La grande vadrouille*, 1966.

C. Exercices du chapitre I

C.1. Exercice (Surjectivité de $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{F}_p)$)

Soit p un nombre premier. Montrer que la réduction modulo p donne un morphisme surjectif $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{F}_p)$.

On a bien un morphisme car la réduction $\mathbb{Z} \to \mathbb{F}_p$ est un morphisme d'anneaux. Pour montrer la surjectivité, on voit, par l'algorithme de Gauss, que toute matrice de $\mathrm{GL}_n(\mathbb{F}_p)$ est produit de matrices de transvections et d'une matrice diagonale. On achève la preuve en utilisant la formule

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

puis, en relevant dans $\mathrm{SL}_n(\mathbb{Z})$.

Coordonnées de Plücker

C.2. Exercice. *On veut caractériser la représentation déterminant et ses puissances (qui sont également des représentations). L'espace $\mathscr{M}_n(\mathbb{K})$ est rapporté à sa base E_{ij} de matrices élémentaires et pour $i \neq j$, $\lambda \in \mathbb{K}$, on note $T_{ij}(\lambda)$ la matrice de transvection $\mathrm{I}_n + \lambda E_{ij}$. On rappelle que l'on peut toujours décomposer toute matrice en un produit de matrices de transvections et d'une matrice diagonale.*

On note δ_k une représentation de $\mathrm{GL}_n(\mathbb{K})$ de dimension 1, c'est-à-dire un morphisme de $\mathrm{GL}_n(\mathbb{K})$ dans $\mathbb{K}^*$, tel que :

$$\delta_k\big(\operatorname{diag}(d_1, \dots, d_n)\big) = d_1^k \times \cdots \times d_n^k$$

pour toute matrice diagonale $\operatorname{diag}(d_1, \dots, d_n)$. On va prouver que $\delta_k = \det^k$.

1. *Montrer que les matrices de transvection sont inversibles et toutes semblables. En déduire qu'elles ont toutes même image, non nulle, par δ_k.*
2. *Montrer que $\delta_k\big(T_{ij}(\lambda)\big) = 1$.*
   On pourra utiliser la relation : $T_{ij}(\lambda)T_{ij}(\mu) = T_{ij}(\lambda + \mu)$.
3. *Conclure.*

C.3. Exercice. *Le but de cet exercice est de généraliser à tout r la formule obtenue sur le lien entre Λ^{n-1} et la comatrice de Λ^1.*

1. *Montrer en utilisant l'exercice précédent que pour tout P dans le groupe $\mathrm{GL}_n(\mathbb{K})$, on a :*
$$\det\big(\Lambda^r(P)\big) = \det{}^{\binom{n-1}{r-1}}(P).$$
2. *Soit $M_r = D_{n-r}\operatorname{com}\big(\Lambda^r(P)\big)D_{n-r}^{-1}$ la matrice constituée des cofacteurs de $\Lambda^r(P)$. Montrer que l'on a :*
$$\Lambda^{n-r}(P) = \det{}^{1-\binom{n-1}{r-1}}(P)M_r.$$

C.4. Exercice (Continuité de im et du plongement de Plücker)

Ici, $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$. On rappelle que la grassmannienne $\mathrm{Gr}_{m,n}$, $m \leqslant n$, est munie de la topologie de l'espace homogène $\mathrm{GL}_n(\mathbb{K})/P$, où P est le stabilisateur d'un m-sous-espace.

1. *Montrer que l'application de l'ouvert $\mathscr{M}^0_{n,m}$ des matrices de rang m de $\mathscr{M}_{n,m}(\mathbb{K})$ (identifié à $\mathrm{Hom}(\mathbb{K}^m, \mathbb{K}^n)$) vers $\mathrm{Gr}_{m,n}$ qui à une matrice associe son image, est continue.*
   On a construit l'homéomorphisme $\mathrm{GL}_n(\mathbb{K})/P \simeq \mathscr{M}^0_{n,m}/\mathrm{GL}_m(\mathbb{K})$ en [H2G2, §IV-3.1].
2. *En déduire que l'on a un homéomorphisme $\mathscr{M}^0_{n,m}/\mathrm{GL}_m(\mathbb{K}) \simeq \mathrm{Gr}_{m,n}$.*
   Cela devrait être contenu dans la preuve du point précédent.
3. *En déduire que le plongement de Plücker est continu.*
4. *Donner une version duale de la question 2 en termes de noyaux, voir [H2G2, théorème IV-2.3].*

C.5. Exercice (Atlas pour la grassmannienne)

Ici, $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$ et l'on fixe $1 \leqslant k \leqslant n$. Pour tout sous-espace G de codimension k dans $\mathbb{K}^n$, on note : $\Omega_G = \{F \in \mathrm{Gr}_{k,n},\ F \oplus G = \mathbb{K}^n\}$. On se propose de montrer que les Ω_G, lorsque G parcourt $\mathrm{Gr}_{n-k,n}$, constituent un recouvrement par des ouverts homéomorphes à des espaces affines.

1. *Montrer en utilisant le théorème 2.13 et la remarque 2.14 que Ω_G est un ouvert de $\mathrm{Gr}_{k,n}$ pour tout G de codimension k.*
2. *Montrer que tout élément de $\mathrm{Gr}_{k,n}$ possède un voisinage de la forme Ω_G pour un espace G convenable.*
3. *On fixe dans la suite les deux supplémentaires $A = \langle e_1, \dots, e_k\rangle$ et $B = \langle e_{k+1}, \dots, e_n\rangle$, où $(e_i)_{1\leqslant i\leqslant n}$ est la base canonique de $\mathbb{K}^n$. À un morphisme f de $\mathscr{L}(A,B)$, on associe son graphe*

$$\mathrm{gr}(f) = \{a + f(a),\ a \in A\} \subset A \oplus B = \mathbb{K}^n.$$

   À un élément F de Ω_B, on associe π_F dans $\mathscr{L}(A,B)$ défini comme la restriction à A de la projection sur B parallèlement à F.
   (a) *Montrer que $\mathrm{gr} : f \mapsto \mathrm{gr}(f)$ et $\pi : F \mapsto \pi_F$ définissent des bijections réciproques entre $\mathscr{L}(A,B)$ et Ω_B.*
   (b) *Quelles sont les coordonnées de Plücker de $\mathrm{gr}(f)$ en fonction de la matrice de f dans les bases naturelles de A et B ?*
   (c) *Déduire que $\mathscr{L}(A,B)$ et Ω_B sont homéomorphes.*
4. *Soit g dans $\mathrm{GL}_n(\mathbb{K})$. Définir un diagramme commutatif d'homéomorphismes :*

$$\begin{array}{ccc} \mathscr{L}(A,B) & \longrightarrow & \mathscr{L}\big(g(A), g(B)\big) \\ {\scriptstyle \mathrm{gr}}\downarrow & & {\scriptstyle \mathrm{gr}}\downarrow \\ \Omega_B & \longrightarrow & \Omega_{g(B)}. \end{array}$$

5. *Conclure.*
   On peut montrer que l'on a en fait un atlas, c'est-à-dire qu'il existe des fonctions de transition régulières entre les deux familles de coordonnées d'un point à l'intersection de deux ouverts du recouvrement.

C.6. Exercice. *Soit E un espace réel de dimension finie muni d'une base $\mathbf{e} = (e_1, \dots, e_n)$. Soient k, p et p', trois entiers tels que l'on ait :*

$$0 < k \leqslant p \leqslant p' \text{ et } p < p + p' - k < n.$$

1. *Soient F_0 le sous-espace de E engendré par $(e_1, \dots, e_{p-1}, e_p)$ et F_0' le sous-espace de E engendré par $(e_{p+1-k}, \dots, e_{p+p'-k})$. Montrer que le sous-espace $G_0 = F_0 \cap F_0'$ est engendré par $(e_{p+1-k}, \dots, e_p)$.*
2. *Montrer que $\dim(F_0) = p$, $\dim F_0' = p'$, $\dim G_0 = k$.*
3. *Soit a un réel* non nul. *On considère le sous-espace F^a de E engendré par $(e_1, \dots, e_{p-1}, e_p + a e_{p+p'-k+1})$. Montrer que $F^a \cap F_0'$ est engendré par $(e_{p+1-k}, \dots, e_{p-1})$ (en particulier, qu'il est nul pour $k = 1$) et que $\dim F^a \cap F_0' = k - 1$. Soit $\mathscr{O}_k$ la partie de $\mathrm{Gr}_p \times \mathrm{Gr}_{p'}$ définie par*

$$\mathscr{O}_k = \big\{(F, F'),\ F \in \mathrm{Gr}_p,\ F' \in \mathrm{Gr}_{p'},\ \dim(F \cap F') = k\big\}.$$

4. *Montrer que $\mathscr{O}_k$ est stabilisé par l'action de $\mathrm{GL}(E)$ sur $\mathrm{Gr}_p \times \mathrm{Gr}_{p'}$.*
5. *Montrer que, pour tout couple (F, F') de $\mathscr{O}_k$, il existe g dans $\mathrm{GL}(E)$ qui envoie (F, F') sur (F_0, F_0').*
   On pourra partir d'une base de $F \cap F'$ et la compléter de façon adéquate en une base de E.
6. *En déduire que les orbites de l'action de $\mathrm{GL}(E)$ sur $\mathrm{Gr}_p \times \mathrm{Gr}_{p'}$ sont les $\mathscr{O}_j$ pour $p + p' - n \leqslant j \leqslant p$.*
   Nous allons montrer que l'intersection fournit une application continue sur $\mathscr{O}_k$. Nous montrerons également que pour la topologie produit sur $\mathrm{Gr}_p \times \mathrm{Gr}_{p'}$, l'adhérence des orbites est donnée par

$$\overline{\mathscr{O}}_k = \bigcup_{k \leqslant j \leqslant p} \mathscr{O}_j.$$

7. *Montrer que l'action de $\mathrm{GL}(E)$ sur $\mathrm{Gr}_p \times \mathrm{Gr}_{p'}$ est continue.*
8. *On considère l'application ι de $\mathscr{O}_k$ dans Gr_k qui envoie (F, F') sur $F \cap F'$. Montrer que cette application est continue pour la topologie produit sur $\mathrm{Gr}_p \times \mathrm{Gr}_{p'}$ et celle de Gr_k.*
   On peut introduire $\bar{\varphi} : \mathrm{GL}(E)/\mathrm{Stab}_{(F_0, F_0')} \to \mathscr{O}_k$, le passage au quotient de $g \mapsto g \cdot (F_0, F_0')$ et commencer par décrire $\iota \circ \bar{\varphi}$.
9. *Montrer que $\mathscr{O}_k \subset \overline{\mathscr{O}}_{k-1}$.*
10. *En déduire l'inclusion $\bigcup_{k \leqslant j \leqslant p} \mathscr{O}_j \subset \overline{\mathscr{O}}_k$.*

11. *Expliquer pourquoi, pour $k' \leqslant n$, l'ensemble des matrices de $\mathscr{M}_{n,p+p'}(\mathbb{R})$ de rang inférieur ou égal à k', est un fermé de $\mathscr{M}_{n,p+p'}(\mathbb{R})$.*

12. *Pour tout couple (g,g') de $\mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{R})$, on associe la matrice $M_{(g,g')}$ de $\mathscr{M}_{n,p+p'}(\mathbb{R})$ dont les colonnes sont données par les vecteurs*

$$g(e_1), \dots, g(e_{p-1}), g(e_p), g'(e_{p+1-k}), \dots, g'(e_{p+p'-k}),$$

dans la base **e** *(on concatène l'image par g de la base fixée de F_0 et l'image par g' de la base fixée de F_0'). En considérant l'application $(g,g') \mapsto M_{(g,g')}$, montrer que l'ensemble des couples (g,g') de $\mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{R})$ tels que $\dim\big(g(F_0) \cap g'(F_0')\big) \geqslant k$ est un fermé.*
On utilisera la formule de Grassmann.

13. *Grâce à l'action du groupe $\mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{R})$ sur $\mathrm{Gr}_p \times \mathrm{Gr}_{p'}$ donnée par $(g,g') \cdot (F,F') = \big(g(F), g'(F')\big)$, montrer enfin l'inclusion inverse : $\overline{\mathscr{O}_k} \subset \bigcup_{k \leqslant j \leqslant p} \mathscr{O}_j$.*

L'orbite fermée $\mathscr{O}_p = \big\{(F,F'),\ F \subset F'\big\}$ est appelée variété d'incidence. *L'exercice qui suit montre qu'il s'agit bien d'une variété algébrique.*

C.7. Exercice. *Soient $1 \leqslant p < p' \leqslant n$. Sur un corps $\mathbb{K}$ quelconque, on note*

$$\mathscr{I} = \big\{(F,F') :\ F \subset F',\ \dim F = p,\ \dim F' = p'\big\} \subset \mathrm{Gr}_{p,n} \times \mathrm{Gr}_{p',n}\,.$$

On veut montrer que $\mathscr{I}$ est caractérisé dans $\mathrm{Gr}_{p,n} \times \mathrm{Gr}_{p',n}$ par les relations suivantes. Pour I, J inclus dans $[1,n]$ avec $|I| = p-1$ et $|J| = p'+1$, soit :

$$\psi_{I,J}(F,F') = \sum_{j \in J \setminus I} (-1)^{\iota(J\setminus\{j\},j)+\iota(j,I)} \Delta_{I\cup\{j\}}(A_F)\Delta_{J\setminus\{j\}}(A_{F'}) = 0.$$

1. *En reproduisant le début de la preuve de l'inclusion directe dans le théorème 2.9, montrer que si (F,F') sont dans $\mathscr{I}$, alors les relations proposées sont satisfaites pour tous I et J.*

2. *Preuve de l'inclusion inverse.*

   (a) *Dans la base canonique (e_i) de $\mathbb{K}^n$, on pose : $F = \langle e_1, \dots, e_p\rangle$ et $F' = \langle e_{r+1}, \dots, e_{r+p'}\rangle$, avec $r > 0$. Montrer que pour $I = \{1, \dots, r-1, r+1, \dots, p\}$, $J = \{r, r+1, \dots, r+p'\}$, la relation correspondant à (I,J) n'est pas vérifiée pour le couple (F,F').*

   (b) *Montrer par la contraposée et en utilisant l'action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathrm{Gr}_{p,n} \times \mathrm{Gr}_{p',n}$ que si $\psi_{I,J}(F,F') = 0$ alors (F,F') est dans $\mathscr{I}$.*

3. *Donner une équation de la variété des drapeaux de $\mathbb{K}^n$ dans le produit $\mathrm{Gr}_{1,n} \times \mathrm{Gr}_{2,n} \times \cdots \times \mathrm{Gr}_{n,n}$.*

Coordonnées de Plücker et algèbre extérieure

C.8. Exercice (*Algèbre extérieure* et somme directe)

On suppose que la caractéristique de $\mathbb{K}$ n'est pas 2. On notera E l'espace $\mathbb{K}^n$ muni de sa base canonique (e_i). On note encore :

$$\Lambda^r(E) = \mathbb{K}^{\Lambda(r,n)} \quad (1 \leqslant r \leqslant n), \quad \Lambda^0(E) = \mathbb{K}, \quad \Lambda^\bullet(E) = \bigoplus_{r=0}^{n} \Lambda^r(E).$$

On munit $\Lambda^\bullet(E)$ d'une structure d'une multiplication graduée, c'est-à-dire compatible avec ses composantes $\Lambda^r(E)$ de degré r, par

$$\begin{array}{rccc} \mu : & \Lambda^r(E) \times \Lambda^{r'}(E) & \longrightarrow & \Lambda^{r+r'}(E) \\ & (v, v') & \longmapsto & w = v \wedge v', \end{array}$$

$$\text{où} \quad w_K = \sum_{I \subset K, |I|=r} (-1)^{\iota(I, K\setminus I)} v_I v'_{K\setminus I} \quad \big(K \in \Lambda(r+r', n)\big).$$

1. *Montrer que μ munit l'espace $\Lambda^\bullet(E)$ d'une structure d'algèbre (non commutative !).*

   Le point clé est l'associativité : on sera amené à montrer que si L, M et N sont disjoints, alors $\iota(L \cup M, N) + \iota(L, M) = \iota(L, M \cup N) + \iota(M, N)$.

2. *Soit $T^\bullet(E)$ l'algèbre libre[22] à n générateurs $X_1, X_2, \ldots, X_n$. Soit I l'idéal engendré par les relations quadratiques $X_i X_j + X_j X_i$, $1 \leqslant i, j \leqslant n$.*

   (a) *Montrer que $T^\bullet(E)/I$ est engendré (comme espace) par les classes de $X_{i_1} X_{i_2} \ldots X_{i_r}$, $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant n$.*

   (b) *Montrer que le morphisme d'algèbres $\phi : T^\bullet(E) \to \Lambda^\bullet(E)$ qui envoie X_i sur $e_i \in \Lambda^1(E)$ est surjectif et passe au quotient par I.*

   (c) *Montrer par un argument de dimension que le morphisme $\bar{\phi}$ induit par passage au quotient est un isomorphisme.*

3. *On note $\mathrm{Gr}_{\bullet,n} = \bigcup_{1 \leqslant k \leqslant n} \mathrm{Gr}_{k,n}$ et l'on considère l'application :*

$$\psi : \mathrm{Gr}_{\bullet,n} \to \mathbb{P}\big(\Lambda^\bullet(E)\big), \ F \mapsto \psi(F).$$

   Soient F et F' deux sous-espaces en somme directe.

   (a) *Montrer que le produit $\psi(F) \wedge \psi(F')$ est bien défini dans $\Lambda^\bullet(E)$.*

   (b) *Montrer que $\psi(F \oplus F') = \psi(F) \wedge \psi(F')$.*

C.9. Exercice. *Montrer qu'un élément $\omega \in \mathbb{P}(\Lambda^2(E))$ représente un plan,* i.e. *appartient à l'image de ψ, si et seulement si $\omega \wedge \omega = 0$.*

[22] Cette algèbre est définie quelque part dans [56]...

C.10. Exercice. *On posera ici $E = \mathbb{K}^n$. On considère l'automorphisme η de l'espace $\Lambda^\bullet(E)$ défini par composantes :*

$$\begin{array}{rccc} \eta : & \Lambda^r(E) & \longrightarrow & \Lambda^{n-r}(E) \\ & v & \longmapsto & w = \eta(v) \end{array}$$

$$\text{avec} \quad \eta(v)_I = (-1)^{\ell(I)} v_{\bar{I}} \quad \big(I \subset [1,n],\ \bar{I} = [1,n] \setminus I\big).$$

On définit un produit $\cdot$ sur $\Lambda^\bullet(E)$ en tordant le produit extérieur $\wedge$ par ι :

$$v \cdot v' = \iota^{-1}\big(\iota(v) \wedge \iota(v')\big).$$

Soient F et F' tels que $F + F' = E$. Montrer que $\psi(F \cap F') = \psi(F) \cdot \psi(F')$.

C.11. Exercice. *On posera ici $E = \mathbb{K}^n$.*

1. *En interprétant la preuve de l'injectivité de ψ en termes de produit extérieur, montrer que si W est un sous-espace de dimension r et $\psi(W) = [\Lambda_W] \in \Lambda^r(E)$, alors on peut retrouver W à partir de Λ_W par*

$$W = \{x \in E,\ \Lambda_W \wedge x = 0\}.$$

2. *Soit $\Lambda \in \Lambda^r(E)$ et soit $W = \{x \in E,\ \Lambda \wedge x = 0\}$. Montrer que si W est de dimension r, alors $[\Lambda] = [\Lambda_W]$, avec Λ_W comme ci-dessus.*
   On peut le montrer d'abord lorsque W est engendré par les r premiers vecteurs de la base canonique, puis utiliser une l'action de $\mathrm{GL}_n(\mathbb{K})$.
3. *Déduire de ce qui précède que l'on peut caractériser l'image de $\psi_{r,n}$ par*

$$[\Lambda] \in \psi(\mathrm{Gr}_{r,n}) \iff \dim\{x \in E,\ \Lambda \wedge x = 0\} = r.$$

C.12. Exercice. *Cet exercice fournit un petit formulaire sur le produit extérieur et le produit intérieur. On verra aussi une version plus conceptuelle des relations de Plücker liée à ces produits. On posera ici $E = \mathbb{K}^n$. Pour tout r, l'espace $\Lambda^r(E)$ est rapporté à la base canonique $(e_I)_{I \in \Lambda(r,n)}$ et $(e_I^*)_{I \in \Lambda(r,n)}$ est la base duale de $\Lambda^r(E)^*$.*

1. *Soient I, J des parties de $[1,n]$. Montrer que l'on a, dans $\Lambda^\bullet(E)$:*

$$e_I \wedge e_J = \begin{cases} (-1)^{\iota(I,J)} e_{I \cup J} & \text{si } I \cap J = \emptyset \\ 0 & \text{sinon.} \end{cases}.$$

2. *Montrer que l'application définie, pour $\omega_i \in E^*$ $(1 \leqslant i \leqslant r)$ et $x_i \in E$ $(1 \leqslant i \leqslant r)$, par :*

$$\omega_1 \wedge \cdots \wedge \omega_r(x_1 \wedge \cdots \wedge x_r) = \sum_{\sigma \in \mathfrak{S}_r} \varepsilon(\sigma) \prod_i \omega_i(x_{\sigma(i)})$$

permet de définir un isomorphisme de $\Lambda^r(E^*)$ vers $\Lambda^r(E)^*$. Montrer que cet isomorphisme est canonique. Montrer que pour $I =\in \Lambda(r,n)$, l'image de e_I est e_I^*.

3. Pour tout ω dans $\Lambda^{r-1}(E^*) \simeq \Lambda^{r-1}(E)^*$, on note

$$ {}^t\omega : \Lambda^r(E) \to \Lambda^1(E) = E $$

la transposée de l'application

$$ E^* \simeq \Lambda^1(E^*) \longrightarrow \Lambda^r(E^*) \simeq \Lambda^r(E)^*, \ \phi \longmapsto \phi \wedge \omega. $$

Montrer que l'on a pour tous $I \in \Lambda(r-1,n)$ et $K \in \Lambda(r,n)$:

$$ {}^t e_I^*(e_K) = \begin{cases} (-1)^{\iota(i,I)} e_i & \text{si } K = I \cup \{i\}, \\ 0 & \text{sinon.} \end{cases} $$

4. Montrer que le polynôme de Plücker peut s'écrire :

$$ \mathscr{P}_{I,J}(x) = e_J^*\big(x \wedge {}^t e_I^*(x)\big), \ x \in \Lambda^r, \ I \in \Lambda(r-1,n), \ J \in \Lambda(r+1,n). $$

Fibrations

Une application continue $\pi : X \to Y$ entre deux espaces topologiques est un *fibré* de fibre F (un autre espace) si, pour tout point $y \in Y$, il existe un voisinage V de y et un homéomorphisme $\pi^{-1}(V) \simeq V \times F$ qui fait commuter le diagramme :

$$ \begin{array}{ccc} \pi^{-1}(V) & \xrightarrow{\sim} & V \times F, \\ & {\scriptstyle \pi} \searrow & \downarrow {\scriptstyle p_1} \\ & & V \end{array} $$

où $p_1 : V \times F \to V$, $(v,f) \mapsto v$ est la première projection. On appelle un ouvert V comme ci-dessus un *ouvert de trivialisation.* C'est que l'exemple le plus simple de fibré, dit *trivial*, est la projection $p_1 : Y \times F \to Y$.

Soit $\mathbb{K}$ un corps, soient k et n deux entiers, avec $1 \leqslant k \leqslant n$. On note $G = \mathrm{GL}_n(\mathbb{K})$, $\mathbf{e} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{K}^n$, P_k le stabilisateur de $\mathbb{K}e_1 + \cdots + \mathbb{K}e_k$ et B le stabilisateur du drapeau standard. On va montrer que les projections naturelles $G \to G/P_k$ et $G \mapsto G/B$ sont des fibrations. Le point crucial est de trouver un ouvert de trivialisation. Il est donné par la décomposition LU (par blocs). Ensuite, on laisse agir le groupe (et ça part tout seul).

C.13. Exercice (Compléments de Schur et fibré)

Soit $g \in G$ une matrice écrite par blocs, celui en haut à gauche étant de taille $k \times k$:

$$ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. $$

On note Ω l'ouvert de G formé des éléments g dont le bloc supérieur gauche a est inversible.

1. *Montrer que pour g dans Ω, il existe $g_1 \in \mathrm{GL}_k(\mathbb{K})$, $r, {}^t h \in \mathscr{M}_{n-k,k}(\mathbb{K})$ et $g_2 \in \mathrm{GL}_{n-k}(\mathbb{K})$ uniques tels que*

$$g = \begin{pmatrix} \mathrm{I}_k & 0 \\ r & \mathrm{I}_{n-k} \end{pmatrix} \begin{pmatrix} g_1 & h \\ 0 & g_2 \end{pmatrix}.$$

On trouve le système : $\begin{cases} a = g_1 \\ b = h \\ c = rg_1 \\ d = rh + g_2, \end{cases}$

qui se résout en : $\begin{cases} g_1 = a \\ h = b \\ r = ca^{-1} \\ g_2 = d - ca^{-1}b. \end{cases}$

2. *Établir la « formule des compléments de Schur » :*

$$\det a \neq 0 \implies \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det(a) \det(d - ca^{-1}b).$$

3. *Déduire de la question 1 un homéomorphisme entre Ω et le produit*

$$R \times P_k, \quad \text{où } R = \left\{ \begin{pmatrix} \mathrm{I}_k & 0 \\ r & \mathrm{I}_{n-k} \end{pmatrix},\ r \in \mathscr{M}_{n-k,k}(\mathbb{C}) \right\}.$$

4. *Soit V l'image de Ω par la projection $\pi_k : G \to \mathrm{Gr}_k(\mathbb{K})$. Justifier que V est un ouvert de la grassmannienne. En donner une caractérisation en termes de coordonnées de Plücker.*
On a vu que π_k est ouverte ; V est décrit par l'inéquation $\Delta_{I_0} \neq 0$, où $I_0 = \{1, \ldots, k\}$.

5. *Montrer enfin que la projection $G \to G/P_k$ est un fibré de fibre P_k.*
On identifie G/P_k à Gr_k, de sorte que la restriction de la projection naturelle à Ω s'identifie à la première projection $R \times P_k \to R$. Pour h dans G, la restriction de la projection naturelle à $h\Omega$ s'identifie à $hR \times P_k \to hR$. Ainsi, les $h\Omega$ forment un recouvrement de G par des ouverts de trivialisation.

C'est un résultat très proche de celui de l'exercice C.5.

C.14. Exercice (Méthode LU et fibration)

Soient B^- le groupe des matrices triangulaires inférieures (on l'appelle sous-groupe de Borel opposé *à B) et U^- le sous-groupe de B formé des éléments unipotents (*i.e. *dont la seule valeur propre est 1). On note w_0 la matrice de la permutation $(1,n)(2,n-1)\ldots$ La* grosse cellule *est Bw_0B.*

1. *Montrer que la multiplication induit un homéomorphisme* $U^- \times B \to Bw_0B$.

   On vérifie d'abord que $B^- = Bw_0$, puis l'on chasse les coefficients diagonaux. C'est une façon d'exprimer la *méthode LU.*

2. *En déduire que* Bw_0B/B *est un ouvert de trivialisation de la projection* $G \to G/B$.

3. *Par principe de translation, en déduire que la projection* $G \to G/B$ *est un fibré de fibre* B.

   Procéder comme dans la question 5 de l'exercice C.13.

Groupe symétrique et variétés de Schubert

C.15. Exercice. *Soit* $w_0 = (1,n)(2,n-1)\dots$ *et soient* $\sigma, \sigma' \in \mathfrak{S}_n$ *tels que* $\sigma' \preceq \sigma$. *Montrer que* $w_0\sigma \preceq w_0\sigma'$.

C.16. Exercice. *On munit* $\mathfrak{S}_n$ *de l'ordre de Bruhat. Pour* $m \in [1,n]$, *on note* $I_m = [1,m]$. *Pour* $k \in [1,n-1]$, *on note* s_k *la transposition simple* $(k,k+1)$. *Soit* σ *une permutation de* $\mathfrak{S}_n$. *On note* $I(w)$ *l'ensemble des couples* $(i,j) \in [1,n]^2$ *tels que* $i<j$ *et* $w(i) > w(j)$.

1. *Remarquer que l'on a :* $ws_k(I_m) = w(I_m)$ *pour* $m \neq k$ *et* $ws_k(I_k) = w(I_k) \setminus \{w(k)\} \cup \{w(k+1)\}$. *En déduire que l'on a :* $w \leqslant ws_k$ *si et seulement si* $w(k) < w(k+1)$.

2. *Montrer que l'on a :* $w \preceq s_kw$ *si et seulement si* $I(w) \subset I(s_kw)$.

3. *Montrer que l'on a :* $w \preceq ws_k$ *si et seulement si* $I(w^{-1}) \subset I(s_kw^{-1})$.

C.17. Exercice

1. *Soient* $A = (a_{ij})$ *une matrice de* $\mathscr{M}_n(\mathbb{K})$ *et* $P_w = (\delta_{iw(j)})$ *la matrice de la permutation* $w \in \mathfrak{S}_n$, *que l'on notera également* w *si aucune ambiguïté n'est possible. Montrer que l'on a :* $P_{w^{-1}}AP_w = (a_{w(i)w(j)})$.

2. *Soient* $G = \mathrm{GL}_n(\mathbb{K})$ *et* B *le sous-groupe des matrices triangulaires supérieures. Montrer que le stabilisateur de* wB *pour l'action par multiplication à gauche de* B *sur* G/B *est*

$$\mathrm{Stab}_B\, wB = \big\{(b_{ij}) \in B,\ b_{ij} = 0 \text{ si } i<j \text{ et } w^{-1}(i) > w^{-1}(j)\big\}.$$

   Le stabilisateur en question est le groupe des matrices inversibles A telles que $P_{w^{-1}}AP_w \in B$.

3. *Déduire de l'exercice C.16 que si* s *est une transposition simple telle que* $w \preceq ws$, *alors on a :* $\mathrm{Stab}_B\, wsB \subset \mathrm{Stab}_B\, wB$.

   Interpréter $\mathrm{Stab}_B\, wB$ à l'aide de $I(w^{-1})$.

4. *Montrer, en utilisant le corollaire A.19, que si* $\ell(uv) = \ell(u)+\ell(v)$, *alors on a :* $\mathrm{Stab}_B\, uvB \subset \mathrm{Stab}_B\, uB$.

L'exercice IV-A.14 donne une application directe de celui-ci au calcul du polynôme générateur des longueurs dans le groupe symétrique.

C.18. Exercice (Action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathscr{B} \times \mathscr{B}$)

Soit G un groupe et soit B un sous-groupe de G. On considère d'une part l'ensemble $B\backslash G/B = \{BgB, g \in G\}$ et l'ensemble $(G/B \times G/B)/G$ des G-orbites pour l'action de G sur $G/B \times G/B$ donnée par $g \cdot (hB, h'B) = (ghB, gh'B)$.

1. *Montrer que toute G-orbite pour l'action sur $G/B \times G/B$ rencontre un unique élément de la forme (B, kB), $k \in G$.*
2. *Montrer que les applications entre $B\backslash G/B$ et $(G/B \times G/B)/G$ données par $BgB \mapsto (B, gB)$ et $G(g_1B, g_2B) \mapsto Bg_1^{-1}g_2B$ sont des bijections.*
3. *On suppose ici que G est le groupe $\mathrm{GL}_n(\mathbb{C})$ et que B est le sous-groupe des matrices triangulaires supérieures, de sorte que G/B est la variété des drapeaux complets $\mathscr{B}$. On munit $\mathscr{B}$ et $\mathscr{B} \times \mathscr{B}$ de la topologie naturelle. Montrer que la bijection envoie, par transport de structure, l'ordre de dégénérescence des B-orbites de $\mathscr{B}$ sur l'ordre de dégénérescence des G-orbites de $\mathscr{B} \times \mathscr{B}$.*

L'identification entre $\mathscr{B}\times\mathscr{B}/G$ et $\mathfrak{S}_n$ est particulièrement féconde. Elle permet de voir naturellement l'algèbre de Hecke, objet fondamental en théorie des représentations, comme une déformation de l'algèbre du groupe symétrique.

C.19. Exercice (Drapeaux en position w)

On garde les notations de l'exercice C.18. Soient B' et B'' deux drapeaux complets de l'espace $\mathbb{K}^n$. Pour w dans $\mathfrak{S}_n$, on dit que le couple (B', B') de $\mathscr{B} \times \mathscr{B}$ est en position w *si (B', B'') est dans la même G-orbite que (B, wB). Soit s une transposition simple dans $\mathfrak{S}_n$. Dans les questions qui suivent, les B_i désignent des drapeaux de $\mathscr{B}$. Cet exercice peut se faire, soit de façon élémentaire, soit à l'aide des algèbres de Hecke.*

1. *On suppose que (B_1, B_2) et (B_2, B_3) sont en position s.*

   (a) *Montrer que (B_1, B_3) est en position s ou en position e.*

   On se ramène à $B_1 = B$, $B_2 = bsB$, avec $b \in B$. Le couple (B_2, B_3) étant en position s, on a $B_3 = bsb'sB$, pour un b' dans B convenable. On utilise le corollaire 4.5 pour montrer l'assertion.

   (b) *Montrer de plus que si $B_1 = B_3$, alors pour tout B_2 tel que (B_1, B_2) est en position s, (B_2, B_3) est aussi en position s.*

Si $B_3 = B$, alors, par translation, le couple (B_2, B_3), avec $B_2 = bsB$, est en position s si et seulement si (B, sB) est en position s, ce qui est vrai pour tout b.

(c) *Montrer que si $B_3 = b'sB$, alors tout drapeau $B_2 = bsB$ vérifie (B_2, B_3) en position s si et seulement si $B_2 \neq B_3$.*

Par translation, il suffit de voir à quelle condition $s^{-1}b^{-1}b'sB \in BsB$. Par le corollaire 4.5, $sb^{-1}b'sB \in BsB$ ou B. Si $s^{-1}b^{-1}b'sB \in B$, alors $B_3 = b'sB = bsB = B_2$.

2. *Soit u un élément de $\mathfrak{S}_n$ tel que $u \preceq su$.*

(a) *Montrer que si (B_1, B_2) est en position s et (B_2, B_3) est en position u, alors (B_1, B_3) est en position su.*

On se ramène par translation au cas où $B_1 = B$, $B_2 = bsB$, avec $b \in B$. Le couple (B_2, B_3) étant en position u, on a $B_3 = bsb'uB$, pour un b' dans B. On utilise donc le corollaire 4.5 pour montrer l'assertion.

(b) *Montrer alors qu'il existe un unique drapeau B_2 tel que (B_1, B_2) soit en position s et (B_2, B_3) en position u.*

Par translation, on se ramène au cas où $B_3 = suB$. On a donc $B_2 = bsB$ et (bsB, suB) est en position u. Par translation, il existe b' dans B tel que $s^{-1}b^{-1}suB = b'uB$. Cela implique que $bsb's^{-1}$ Stab(suB), qui par l'hypothèse $u \preceq su$ et, grâce à l'exercice C.17, donne $bsb's^{-1} \in$ Stab(sB), puis $B_2 = bsB = sB$.

C.20. Exercice (*Variété de Bott-Samelson* et *désingularisation de Demazure* des variétés de Schubert)

Soit $w = s_{i_1}s_{i_2}\cdots s_{i_k}$ une décomposition réduite de la permutation $w \in \mathfrak{S}_n$ en transpositions simples. On pose $\mathbf{i} = (i_1, i_2, \ldots, i_k)$ et $P_{\mathbf{i}} = P_{i_1} \times P_{i_2} \cdots \times P_{i_k}$, où $P_i = B \cup Bs_iB$ est le sous-groupe parabolique minimal *associé à i. On fait agir le groupe B^k sur $P_{\mathbf{i}}$ par*

$$(b_1, \ldots, b_k) \cdot (p_1, \ldots, p_k) = (p_1b_1^{-1}, b_1p_2b_2^{-1}, \ldots, b_{k-2}p_{k-1}b_{k-1}^{-1}, b_{k-1}p_kb_k^{-1}).$$

Enfin, on considère le quotient $Z_{\mathbf{i}} = P_{\mathbf{i}}/B^k$ appelé variété de Bott-Samelson.

1. *Montrer que l'application μ qui envoie $(p_1, p_2, \ldots, p_k)$ sur $p_1p_2\cdots p_kB$ passe au quotient pour définir une application $\bar{\mu}$ de $Z_{\mathbf{i}}$ dans $\mathscr{B}_w$.*

Le passage au quotient est clair. On voit que l'image de μ est dans $\mathscr{B}_w$ grâce au corollaire 4.5 et à une récurrence.

2. *Montrer que $\bar{\mu}$ est surjective.*

On a, par le corollaire 4.5, que $u \preceq su$ implique $BsBuB = BsuB$. On peut alors se servir du fait que tout $w' \preceq w$ possède une décomposition réduite de la forme $s_{i_{\ell_1}}s_{i_{\ell_2}}\cdots s_{i_{\ell_r}}$, pour une suite croissante $\ell_1 < \ell_2 < \cdots < \ell_r$ de $[1, k]$, voir la proposition A.15.

3. *Montrer enfin que $\bar{\mu}$ définit une bijection de $\bar{\mu}^{-1}(BwB)$ sur BwB.*
   On peut utiliser le dernier point du corollaire 4.7.
4. *Cas particulier. On suppose que $k \mapsto i_k$ est injective. Montrer que $\bar{\mu}$ est bijective.*

Comme pour la désingularisation de Springer, voir le §II-3, la variété de Bott-Samelson est une « désingularisation » de la variété de Schubert dans le sens qu'elle est « lisse » (sans singularité), qu'elle se projette surjectivement sur la variété de Schubert, et que cette surjection est bijective sur un ouvert dense. On peut donc la voir comme étant la variété lisse la plus proche de la variété de Schubert.

C.21. Exercice (Groupe simple d'ordre 168 et décomposition à la Bruhat)

Voici une application de la décomposition de Bruhat à la preuve (inachevée) qu'il existe un unique groupe simple d'ordre 168. *Soit donc G un groupe simple d'ordre* $168 = 2^3 \times 3 \times 7$. *On veut montrer qu'il possède une décomposition disjointe $G = B \cup BsN$, où N est un p-groupe et B est le normalisateur de N dans G.*

1. *Montrer que G possède exactement huit 7-Sylow. On en fixe un, N.*
2. *En déduire que G s'injecte dans le groupe $\mathfrak{S}_8$.*
3. *Soit B le normalisateur de N dans G.*
   (a) *Montrer avec les théorèmes de Sylow que l'on a : $|B| = 168/8 = 21$.*
   (b) *Montrer, en injectant B dans $\mathfrak{S}_8$, que B n'est pas abélien. Puis, en déduire que B est isomorphe au produit semi-direct $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$.*
4. *Soit s un élément s d'ordre 2 de G.*
   (a) *Vérifier que s n'appartient pas à B.*
   (b) *En déduire que l'on a : $B \cap BsN = \emptyset$.*
   (c) *En déduire aussi que l'on a : $sNs^{-1} \cap B = \{1\}$.*
   Comme sNs^{-1} est d'ordre 7, $sNs^{-1} \cap B$ est d'ordre 1 ou 7. Si c'était 7, alors sNs^{-1} serait un 7-Sylow du groupe B. Par unicité, puisque N est distingué dans B, on aurait $sNs^{-1} = N$, et donc $s \in B$.
   (d) *Montrer par ce qui précède que l'application de $B \times N$ dans BsN qui envoie (b, n) sur bsn est bijective.*
   (e) *Déduire enfin la décomposition voulue : $G = B \cup BsN$.*
5. *Montrer que dans le cas $G = \mathrm{PSL}_2(\mathbb{F}_7)$, on retrouve à conjugaison près la projection de la décomposition de Bruhat.*

On peut montrer avec un peu plus de travail et en distinguant quatre cas, selon que g et g' sont dans B ou dans BsN, que gg' est « complètement déterminé » par B et N et donc qu'il n'y a qu'un seul groupe simple d'ordre 168 *à isomorphisme près. En particulier, on a :* $\mathrm{PGL}_2(\mathbb{F}_7) \simeq \mathrm{GL}_3(\mathbb{F}_2)$. *Voir les détails de la preuve dans [80, §2, Exemple 4]. On trouve une autre preuve, plus simple, dans [65], en exercice dans le chapitre IV.*

Présentation de Coxeter du groupe symétrique

C.22. Exercice (Automorphisme extérieur de $\mathfrak{S}_6$, première !)

La figure C.1 est une « preuve sans mots » de l'existence d'un automorphisme extérieur de$\mathfrak{S}_6$. *On rappelle que le groupe de Klein $\mathfrak{K}$, engendré par les double-transpositions de $\mathfrak{S}_4$, est commutatif.*

1. *Vérifier qu'il y a dans $\mathfrak{S}_6$ autant de transpositions que de triples transpositions (produits de trois transpositions de supports disjoints).*
   On sait que tout automorphisme qui envoie une transposition sur une transposition est intérieur. Cette coïncidence numérique rend donc possible l'existence d'un automorphisme extérieur.
2. *Montrer que les triples transpositions $t_1, \ldots, t_5$ de la figure C.1 satisfont aux relations de $s_1 = (12), \ldots, s_5 = (56)$, voir la proposition B.7.*

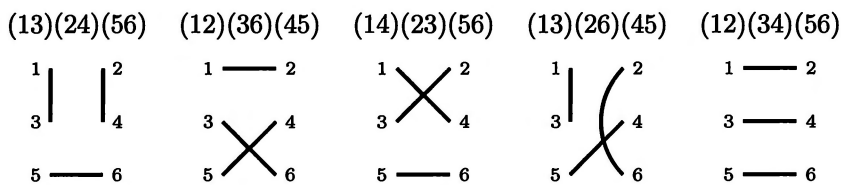


Figure C.1. *Présentation de Coxeter de $\mathfrak{S}_6$ par triples transpositions*

Si $|i-j| \geqslant 2$, la commutation de t_i et t_j se voit parce que les diagrammes ont une arête commune, ce qui ramène à la commutativité du groupe de Klein. Pour les relations de tresses, on voit que $t_i t_{i+1}$ est d'ordre 3 parce qu'il est produit de deux 3-cycles disjoints, si l'on se rappelle que $(ab)(bc) = (abc)$.

3. *Avec la propriété universelle d'une présentation de groupe, montrer que l'application $s_i \mapsto t_i$ $(i = 1, \ldots, 5)$ s'étend en un automorphisme extérieur de $\mathfrak{S}_6$.*

Merci à Olivier Mathieu de nous avoir suggéré cet exercice.

C.23. Exercice (Élément de plus grande longueur)

Soit n un entier naturel non nul et soit w_0 la permutation de $\mathfrak{S}_n$ qui échange i et $n+1-i$ $(1 \leqslant i \leqslant n)$.

1. *Vérifier une fois de plus que tout couple (i,j) avec $i<j$ est une inversion de w_0 et que $w_0 = s_1 s_2 s_1 s_3 s_2 s_1 \cdots s_{n-1} s_{n-2} \cdots s_2 s_1$. Retrouver ainsi, de deux façons différentes, que l'on a : $N(w_0) = n(n-1)/2 = \ell(w_0)$.*
2. *Soit $w \in \mathfrak{S}_n$. Vérifier que l'on a : $I(w_0 w) \cap I(w) = \Phi$. En déduire la relation : $\ell(w_0 w) + \ell(w) = n(n-1)/2$.*
3. *Soit $w \in \mathfrak{S}_n$. Montrer que l'on a : $\ell(w w_0) = \ell(w_0) - \ell(w) = \ell(w_0 w)$.*

C.24. Exercice (Signature à mains nues)

Soit n un entier supérieur à 1. Soit P l'ensemble des paires (parties à deux éléments) de $\{1,\dots,n\}$. Pour $w \in \mathfrak{S}_n$, on note P_w l'ensemble des paires $p = \{i,j\}$ telle que $i<j$ et $w(i) > w(j)$ (ainsi, si $i<j$, $\{i,j\} \in P_w$ si et seulement si $(i,j) \in I(w)$).

1. *Étant données deux parties finies A et B,on note $A \triangle B$ leur différence symétrique. Vérifier que l'on a : $|A \triangle B| = |A| + |B| - 2|A \cap B|$.*
2. *Soit $w \in \mathfrak{S}_n$ et soit $p \in P$, disons $p = \{i,j\}$ avec $i<j$. Vérifier que $p \in P_w$ si et seulement si la restriction de w à p est croissante si et seulement si (i,j) est une inversion de w.*
3. *Soient $w, w' \in \mathfrak{S}_n$. Montrer que l'on a : $P_{w'w} = P_w \triangle w^{-1}(P_{w'})$.*
4. *Conclure : l'application $\varepsilon : w \mapsto (-1)^{|P_w|}$ est un morphisme non trivial de groupes.*

Cet exercice est tiré de la note [62].

C.25. Exercice (Unicité de la signature)

Soit n un entier naturel non nul.

1. *À l'aide du principe de conjugaison, montrer que toutes les transpositions sont conjuguées.*
2. *Le redémontrer à l'aide de la présentation de Coxeter.*
3. *Soit $\varphi : \mathfrak{S}_n \to \mathbb{C}^*$ un morphisme de groupes. En utilisant le fait que $\mathbb{C}^*$ est abélien, montrer que φ est le morphisme trivial ou la signature, selon que l'image de la transposition (12) vaut 1 ou pas.*

C.26. Exercice (« Racines négativées »)

Soit $w \in \mathfrak{S}_n$. On suppose que $w = s_{i_1} \cdots s_{i_\ell}$, où $\ell = \ell(w)$. Alors :

$$I(w) = \{ s_{i_\ell} \cdots s_{i_{r+1}} (i_r, i_r+1) \,:\, 1 \leqslant r \leqslant \ell \}.$$

Procéder par récurrence sur ℓ. Si $w' = w s_{i_\ell}$, décrire $I(w')$ et montrer que $I(w) = s_{i_\ell} I(w') \cup \{(i_\ell, i_\ell+1)\}$.

C.27. Exercice (Présentation alternative du groupe $\mathfrak{S}_n$)

Soit $n \geqslant 2$. On note G_n présenté par générateurs $(x_i)_{1 \leqslant i \leqslant n-1}$ et relations :

$$\begin{cases} x_i^2 = e & \text{pour tout } i, \\ x_i x_j x_i = x_j x_i x_j & \text{pour tous } i, j \text{ distincts}, \\ (x_i x_j x_i x_k)^2 = e & \text{pour tous } i, j, k \text{ deux à deux distincts.} \end{cases}$$

1. *Montrer qu'il existe un morphisme surjectif $G_n \to \mathfrak{S}_n$, $x_i \mapsto (1, i+1)$ $(1 \leqslant i \leqslant n-1)$.*

   Par la propriété universelle des groupes libres, il existe un morphisme de L_{n-1} qui envoie les $n-1$ générateurs sur les $n-1$ transpositions $(1, i+1)$ de $\mathfrak{S}_n$. Comme ces transpositions constituent un système de générateurs de $\mathfrak{S}_n$, le morphisme est surjectif. On vérifie que ces transpositions satisfont aux relations imposées pour passer au quotient.

2. *Soit H le sous-groupe engendré par $x_1, \ldots, x_{n-2}$. Montrer que l'on a :*

$$G_n = H \cup x_{n-1}H \cup x_1 x_{n-1} H \cup \cdots \cup x_{n-2} x_{n-1} H.$$

   On montre, à la sueur de son front, au cas par cas et en utilisant les relations, que $H \cup x_{n-1}H \cup x_1 x_{n-1} H \cup \cdots \cup x_{n-2} x_{n-1} H$ est une partie de G_n contenant e et stable par multiplication à gauche par tous les x_i. Cela assure l'égalité. Voici un exemple de cas : lorsque l'on multiplie à gauche x_j $(1 \leqslant j \leqslant n-2)$ par un élément de $x_i x_{n-1} H$ $(1 \leqslant i \leqslant n-2)$, on obtient un élément de $x_j x_i x_{n-1} H$, qui par la dernière relation et le fait que les x_k sont d'ordre 2, vaut $x_i x_{n-1} x_i x_j x_i H = x_i x_{n-1} H$. Tout le reste est à l'avenant.

3. *Montrer par récurrence que G_n est isomorphe à $\mathfrak{S}_n$.*

   Par hypothèse de récurrence, H est isomorphe à $\mathfrak{S}_{n-1}$ donc le cardinal de G_n est au plus $n \times |H| = n!$. Vu la surjection de G_n sur $\mathfrak{S}_n$, l'inégalité inverse est vraie et la surjection de $G_n \to \mathfrak{S}_n$ est un isomorphisme.

The eagle never lost so much time
as when he submitted to learn from the crow.
Jim Jarmusch, *Dead man*, 1995.

Chapitre II

Réduction des endomorphismes

Voici les dernières histoires (hédonistes) en date sur les endomorphismes. Peut-être était-il temps d'en finir avec cette thématique qui nous poursuivait depuis le début de la licence. En fait, le coup fatal lui a déjà été porté avec les invariants de similitude, voir [H2G2, corollaire III-5.10] ; ces objets permettent d'identifier formellement si deux matrices d'endomorphismes sont, ou non, dans la même classe de similitude. Reste maintenant à affiner les deux notions phares de la réduction : la diagonalisabilité[1] et la nilpotence.

Pour la première notion, on introduit la semi-simplicité. Il s'agit là d'une généralisation de la diagonalisabilité, qui est stable (du moins en caractéristique zéro ou sur un corps fini) par passage aux sous-corps admissibles, c'est-à-dire sur lesquels la matrice reste définie. En revanche, ce n'est pas un enjeu pour la nilpotence, notion complètement indépendante du corps de base. Là, l'étude relèvera de la géométrie algébrique et plus précisément l'étude des singularités. On remarquera que l'ensemble des matrices nilpotentes sur un corps donné forme un « vrai » cône, qui n'est certainement pas un sous-espace vectoriel de l'espace des matrices. Ainsi, il possède une singularité (une pointe, disons) en l'origine, et de plus, l'action du groupe des homothéties permet de voir qu'un voisinage de cette pointe en l'origine résume toute l'information, en particulier toutes les singularités, que l'on peut trouver sur le cône. L'idée est alors de construire un objet régulier, *i.e.* sans singularité, qui se rapproche le plus de ce cône : il s'agit de la désingularisation du cône nilpotent. Vu que la théorie des singularités est assez

[1] D'expérience, un des mots les plus difficiles à prononcer pour les candidats le jour de l'oral d'algèbre. Une séance de lentes inspirations et quelques exercices de diction trouveront toute leur utilité.

éloignée de nos prérequis, nous n'en dirons finalement pas grand-chose, mais l'histoire reste instructive et plaisante.

Le troisième thème du chapitre porte sur le commutant d'un endomorphisme. Nous verrons qu'une compréhension assez précise peut résulter des invariants de similitude. Nous introduirons également le *bicommutant*, plus « stable » que le commutant, puisqu'il ne dépend que du polynôme minimal de l'endomorphisme en question.

Que ceux qui se désespéreraient de voir ainsi se tarir une si belle thématique sachent qu'il ne s'agit nullement d'une fin. Ne dit-on pas que les étoiles ne meurent jamais car elles restent au firmament ? L'annexe sur les modules permet d'entrevoir une suite possible, une théorie qui prolonge celle de la réduction des endomorphismes. Elle interviendra d'ailleurs avec force dans le chapitre suivant à travers les algèbres de carquois.

1. Semi-simplicité

Comme [H2G2, §III-5.3], on dit qu'un espace vectoriel[2] E muni d'un endomorphisme u est *u-cyclique* s'il existe un vecteur x de E tel que $E = \mathbb{K}[u]\cdot x$. On dit aussi que l'endomorphisme u est *cyclique*. On a vu qu'un endomorphisme est cyclique si et seulement si son polynôme minimal est égal à son polynôme caractéristique. Cela implique, entre autres, que la propriété d'être cyclique est stable par extension de corps, puisque le polynôme caractéristique et le polynôme minimal le sont[3].

Sur un corps quelconque, les endomorphismes cycliques sont classés à similitude près par leur seul invariant de similitude : leur polynôme caractéristique. Il est amusant de voir qu'à l'opposé[4], les endomorphismes diagonalisables sur un corps algébriquement clos sont caractérisés par leur spectre, c'est-à-dire également par leur polynôme caractéristique. Mais la propriété d'être diagonalisable n'est pas invariante par descente à un sous-corps.

Ici, on introduit la notion de *semi-simplicité* : sur un corps algébriquement clos, les endomorphismes semi-simples sont ceux qui sont diagonalisables mais la notion est stable par extension de corps. On retrouvera avec le théorème de Maschke X-A.12 une notion proche pour les représentations de groupes finis.

---

[2]Sauf mention du contraire, les espaces sont supposés de dimension finie.

[3]C'est clair pour le polynôme caractéristique ; pour le polynôme minimal, on l'a vu à la [H2G2, remarque III-5.2].

[4]Dans l'ensemble des matrices qui ont un polynôme caractéristique donné, on peut montrer que les matrices semblables à une matrice compagnon forment une orbite ouverte ; à l'opposé, on sait les diagonalisables forment une orbite fermée. Mais très souvent, ce sont les mêmes.

Avant de commencer, il est bon de se remémorer le théorème de décomposition de Frobenius, [H2G2, théorème III-5.7], qui introduit les *invariants de similitude* d'un endomorphisme, ou *facteurs invariants.*

1.1. Théorème. *Soit u un endomorphisme d'un espace vectoriel E sur un corps $\mathbb{K}$. Alors, il existe un unique entier naturel s et une unique famille de polynômes unitaires non constants $(F_1, \dots, F_s)$ de $\mathbb{K}[X]$ tels que :*

(i) $F_s \mid F_{s-1} \mid \cdots \mid F_1$,

(ii) $E = \bigoplus_{k=1}^{s} \mathbb{K}[u] \cdot x_k$, *où x_k est un élément tel que F_k est le générateur unitaire de l'idéal $\{P \in \mathbb{K}[X],\ P(u) \cdot x_k = 0\}$.*

On peut aussi se rapporter à [H2G2, corollaire III-5.9] pour interpréter ce théorème en disant que E se décompose en somme directe de sous-espaces u-cycliques, ou, que la matrice de u peut s'écrire matriciellement par blocs diagonaux de matrices compagnon.

1.2. Définition. Soit u un endomorphisme de l'espace vectoriel E *non nul* sur $\mathbb{K}$. On dit que u est *simple* ou que E est *u-simple* si les seuls sous-espaces u-stables de E sont $\{0\}$ et E.

Sur $\mathbb{C}$, les seuls endomorphismes simples sont en dimension 1, puisque $\mathbb{C}$ est algébriquement clos et ainsi, tout endomorphisme admet une droite propre. Sur $\mathbb{R}$, on trouve des endomorphismes simples en dimension 1 et 2 (par exemple, une rotation d'angle non multiple de π du plan réel). On constate dans ces deux cas que la liste des dimensions est aussi la liste des degrés des polynômes irréductibles. Et pour cause.

1.3. Proposition. *Un endomorphisme est simple si et seulement si son polynôme caractéristique est irréductible.*

Démonstration. Soit F un sous-espace de E stable par u. En complétant une base de F en une base de E, on obtient une matrice de u de la forme

$$\begin{pmatrix} A & B \\ 0 & A' \end{pmatrix}$$

et donc une polynôme caractéristique de u : $\chi_u = \chi_A \chi_{A'}$. Si χ_u est irréductible, F est soit nul, soit E tout entier.

Réciproquement, si u est simple, alors le sous-espace engendré par un vecteur non nul et ses images par les puissances successives de u est E tout entier, de sorte que u est cyclique et ne possède qu'un seul facteur invariant F_1 (on avait déjà vu cette propriété au [H2G2, corollaire III-5.9]). Cela

implique que F_1 est à la fois son polynôme minimal μ_u et son polynôme caractéristique χ_u[5].

Soit P un facteur irréductible de μ_u. Écrivons $\mu_u = P^k Q$ avec k entier non nul et Q premier à P. Par le lemme des noyaux, l'espace E se décompose comme somme directe des noyaux de $P^k(u)$ et de $Q(u)$. Par simplicité, l'un de ces deux espaces est nul. Ce n'est pas le noyau de $P^k(u)$, sinon le polynôme Q annulerait u et serait de degré strictement plus petit que le polynôme minimal μ_u. Ainsi, le noyau de $P^k(u)$ est E entier et, par minimalité de μ_u, on a : $\mu_u = P^k$. Ainsi, $P(u)^k = P^k(u) = 0$ et, comme $P(u)$ est nilpotent, le noyau de $P(u)$ n'est pas réduit à $\{0\}$ et il est stable par u. C'est donc E tout entier, par simplicité. Ainsi, le polynôme irréductible P annule u et, par minimalité de μ_u, on a : $\mu_u = P$. □

La proposition suivante a été utile dans la preuve précédente.

1.4. Proposition. *Tout endomorphisme simple est cyclique.*

Voici donc maintenant une définition de la semi-simplicité qui n'est pas forcément la plus maniable, mais qui possède toutefois des vertus étymologiques illuminantes.

1.5. Définition. Un endomorphisme u est dit *semi-simple* si l'espace E se décompose en somme directe de sous-espaces stables E_i tels que la l'endomorphisme induit u_{E_i} par u sur E_i soit simple pour tout i.

Par exemple, un endomorphisme diagonalisable est semi-simple : on prend pour E_i des droites propres. Voici quelques reformulations de la définition.

1.6. Proposition. *Soit u un $\mathbb{K}$-endomorphisme de E. Alors, les conditions suivantes sont équivalentes :*

(i) *l'endomorphisme u est semi-simple ;*

(ii) *le polynôme minimal de u n'a pas de multiplicité dans sa décomposition en irréductibles de $\mathbb{K}[X]$;*

(iii) *aucun facteur invariant de u n'a de multiplicité dans sa décomposition en irréductibles de $\mathbb{K}[X]$;*

(iv) *pour tout sous-espace u-stable F, l'endomorphisme induit u_F par u sur F est semi-simple ;*

(v) *tout sous-espace u-stable possède un supplémentaire u-stable.*

Si de plus $\mathbb{K}$ est de caractéristique zéro, il est encore équivalent de dire :

(vi) *l'endomorphisme u est diagonalisable sur la clôture algébrique de $\mathbb{K}$.*

[5] On peut se passer de l'argument des facteurs invariants en montrant par le calcul que le polynôme minimal d'une matrice compagnon est égal à son polynôme caractéristique, voir [H2G2, proposition III-5.5].

Démonstration. (i)⇒(ii). Supposons que l'espace E est somme directe de sous-espaces u-stables simples E_i et donc les polynômes minimaux P_i de u_{E_i} sont irréductibles. Soit P le ppcm des P_i, *i.e.* le produit des P_i sans compter de multiplicité. Alors, $P(u)$ s'annule sur E. Cela implique (ii).

(ii)⇒(i). Cela vient du lemme des noyaux et de la proposition 1.3.

(ii)⇔(iii). Cela vient de ce que le premier facteur invariant est le polynôme minimal et que les autres le divisent.

(ii)⇒(iv). Il suffit de remarquer que si F est stable par u, le polynôme minimal de u annule la restriction u_F. Mais alors, la factorisation du minimal de v est sans multiplicité donc v est semi-simple d'après ce qui précède.

(iv)⇒(v). Soit $F \subset E$ un sous-espace u-stable et soit $x \notin F$. Posons alors $F' = \mathbb{K}[u] \cdot x$. Par hypothèse, comme F' est u-stable, il est semi-simple et donc F' est somme directe de sous-espaces u-simples G_i. Pour tout i, on choisit x_i non nul dans G_i. Par simplicité, le sous-espace u-stable engendré par x_i est donc le sous-espace G_i. Si tous les x_i appartenaient à F, alors tous les G_i seraient inclus dans F et l'on aurait $F' \subset F$, ce qui est absurde. Soit donc i tel que $x_i \notin F$. Alors, $\mathbb{K}[u] \cdot x_i \cap F$ est un sous-espace u-stable de $\mathbb{K}[u] \cdot x_i$ distinct de $\mathbb{K}[u] \cdot x_i$. Il est donc nul par simplicité, et $F \oplus G_i$ sont en somme directe. On obtient l'assertion désirée par une récurrence finie, en remplaçant à chaque étape F par $F \oplus G_i$.

(v)⇒(i). Comme on est en dimension finie, un sous-espace u-stable de dimension minimale non nulle est simple. En appliquant la propriété (v) du supplémentaire et une récurrence sur la dimension de E, on obtient la semi-simplicité.

(ii)⇔(vi). D'une part, on sait que le polynôme minimal est invariant par extension de corps ([H2G2, remarque III-5.2] ou [H2G2, corollaire III-5.11]). D'autre part, le fait de ne pas avoir de multiplicité dans sa décomposition en irréductibles est aussi invariant par extension de corps en caractéristique nulle. En effet, un polynôme P est sans multiplicité si et seulement si le résultant $\mathrm{Res}(P, P')$ est non nul et le résultant se calcule dans n'importe quel corps. On peut aussi dire que l'algorithme d'Euclide montre que si P non constant dans $\mathbb{K}[X]$, alors le pgcd de P et P' (ce dernier est non nul en caractéristique zéro) est invariant par extension de corps. □

En fait, la dernière assertion reste vraie plus généralement sur un *corps parfait*[6], voir [46]. Néanmoins, la situation se complique sur un corps non parfait.

[6]Rappelons qu'un corps est dit *parfait* si tout polynôme irréductible est séparable, c'est-à-dire s'il possède une racine multiple dans une extension, c'est-à-dire s'il est premier avec son polynôme dérivé.

1.7. Exemple (Corps non parfait). L'archétype de corps non parfait est le corps de fractions rationnelles $\mathbb{K} = \mathbb{F}_p(T)$, où p est un nombre premier fixé et T est une indéterminée. Le polynôme $X^p - T \in \mathbb{K}[X]$ est irréductible, mais, dès que l'on adjoint une racine t de $X^p - T$ à $\mathbb{K}$, on les obtient toutes. En effet, le corps de rupture de $X^p - T$ est $\mathbb{L} = \mathbb{F}_p(t)$ (isomorphe à $\mathbb{K}$), dans lequel $\mathbb{K}$ s'injecte via $T = t^p$ et l'on a dans $\mathbb{L}[X]$:

$$X^p - T = X^p - t^p = (X - t)^p.$$

Prenons alors pour matrice la matrice-compagnon du polynôme $X^p - T$:

$$A = \begin{pmatrix} 0 & \cdots & 0 & T \\ 1 & & \vdots & 0 \\ & \ddots & 0 & \vdots \\ 0 & & 1 & 0 \end{pmatrix}.$$

Vue dans $\mathscr{M}_p(\mathbb{K})$, la matrice A est semi-simple et même simple, car son polynôme caractéristique est irréductible : c'est $X^p - T$. Mais, dans $\mathscr{M}_p(\mathbb{L})$, la matrice A possède pour polynôme caractéristique $(X - t)^p$, qui est scindé mais pas irréductible. Ainsi, A possède une seule valeur propre, mais n'est pas diagonale, donc A n'est pas diagonalisable.

En particulier, sur un corps parfait, la notion de semi-simplicité est invariante par extension : si $\mathbb{L}/\mathbb{K}$ est une extension de corps et si $\mathbb{K}$ est parfait, une matrice à coefficients dans $\mathbb{K}$ est semi-simple si et seulement si elle l'est quand on la considère comme matrice à coefficients dans $\mathbb{L}$.

2. Commutant

Le commutant $\mathscr{C}_u$ d'un endomorphisme u de E est l'ensemble des endomorphismes qui commutent avec u, c'est-à-dire l'ensemble des solutions de l'équation en v suivante : $vu = uv$. Cette définition, si elle peut paraître simple, ne reflètent pas le caractère naturel et fondamental de l'objet. Pour le voir, un peu de structure comme dans [H2G2, §III-5] ou l'annexe A : la donnée d'un espace E muni d'un endomorphisme u est équivalente à la donnée d'une structure de $\mathbb{K}[X]$-*module* sur E, via $P \cdot x = P(u)(x)$ ($P \in \mathbb{K}[X]$, $x \in E$). La notion de morphisme de $\mathbb{K}[X]$-module est naturelle : il s'agit des applications additives qui commutent avec l'action de $\mathbb{K}[X]$. Le commutant de u n'est autre que l'ensemble des endomorphismes du $\mathbb{K}[X]$-module E. Ainsi, cela pourra en éclairer certains de noter $\mathrm{End}_{\mathbb{K}[X]}(E)$ le commutant de E.

On peut remarquer également que le groupe des inversibles du commutant de u est le stabilisateur de u pour l'action de $\mathrm{GL}(E)$ par conjugaison.

On vérifie sans peine que $\mathscr{C}_u$ est une sous-algèbre de $\mathrm{End}_{\mathbb{K}}(E)$; cette partie sera consacrée à l'étude de cette sous-algèbre. Nous verrons dans quelle mesure le commutant d'un endomorphisme dépend de tous ses facteurs invariants. Nous montrerons enfin un résultat étonnant, du moins au premier abord, selon lequel le bicommutant (les endomorphismes qui commutent avec le commutant) est une algèbre égale à $\mathbb{K}[u]$, et donc ne dépendant que du polynôme minimal.

Tout d'abord, comme tout polynôme en u commute avec u, l'algèbre commutative $\mathbb{K}[u]$ est une sous-algèbre de $\mathscr{C}_u$. Si l'on prend pour u une homothétie, alors $\mathscr{C}_u$ est l'algèbre $\mathrm{End}(E)$ toute entière, de sorte que l'inclusion peut être stricte. En fait, on peut facilement deviner (et cela sera précisé plus tard), à partir de la proposition suivante que la dimension de l'algèbre $\mathscr{C}_u$ ne dépend que du nombre de facteurs invariants de u et de leur degré. Cela n'étonnera guère le lecteur qui aura noté qu'à isomorphisme d'algèbres près, $\mathscr{C}_u$ ne dépend que de la classe de similitude de u.

2.1. Le commutant dans le cas cyclique

2.2. Proposition. *L'espace E est u-cyclique (et donc ne possède qu'un seul facteur invariant) si et seulement si $\mathbb{K}[u] = \mathscr{C}_u$.*

Démonstration. Comme dans [H2G2, lemme III-5.1], pour $x \in E$, on note $\mu_{u,x}$ le générateur unitaire de l'idéal des polynômes P tels que $P(u)(x) = 0$.

Supposons que E est u-cyclique. Par [H2G2, proposition III-5.5], on peut trouver un vecteur $x \in E$ tel que les vecteurs suivants forment une base de l'espace E :

$$\mathbf{x} = \big(x, u(x), \dots, u^{n-1}(x)\big).$$

Soit v dans $\mathscr{C}_u$. On écrit dans la base $\mathbf{x}$, disons : $v(x) = \sum_{k=0}^{n-1} a_k u^k(x)$. À présent, comme v commute avec u, on a pour tout entier m l'égalité : $v\big(u^m(x)\big) = \sum_{k=0}^{n-1} a_k u^k\big(u^m(x)\big)$. On a ainsi : $v(y) = \sum_{k=0}^{n-1} a_k u^k(y)$ pour y dans la base $\mathbf{x}$, donc pour y quelconque. D'où : $v = \sum_{k=0}^{n-1} a_k u^k \in \mathbb{K}[u]$.

Réciproquement, si l'on a l'égalité $\mathbb{K}[u] = \mathscr{C}_u$, montrons par l'absurde que E est u-cyclique. Si ce n'était pas le cas, on aurait une décomposition en $s > 1$ sous-espaces cycliques : $E = \bigoplus_{k=1}^{s} \mathbb{K}[u] \cdot x_k$, avec $\mu_{u,x_k} = F_k$ et $F_s \mid F_{s-1} \mid \cdots \mid F_1$. Soit p_s la projection sur le sous-espace cyclique $\mathbb{K}[u] \cdot x_s$ parallèlement aux autres. Le fait que les sous-espaces cycliques de la décomposition sont u-stables donne immédiatement que p_s commute avec u. Donc, par hypothèse, on peut écrire $p_s = Q(u)$ pour un polynôme Q convenable. Comme $Q(u)$ s'annule sur x_1, le facteur invariant F_1 divise Q. Mais alors, F_s divise Q, de sorte que $p_s = Q(u)$ s'annule sur x_s, absurbe[7].□

[7] By courtesy of the *Rubrik of the brac.*

2.3. Cas général. Dimension du commutant

On vient de voir dans la preuve que les endomorphismes de $\mathbb{K}[u]\cdot x$ qui commutent avec l'action de u forment une algèbre isomorphe à $\mathbb{K}[v]$, où v est l'endomorphisme induit $v = u_{\mathbb{K}[u]\cdot x}$, et donc cette algèbre est isomorphe à $\mathbb{K}[X]/(\mu_{u,x})$. Étendons ce résultat à un espace non cyclique. Si l'on a une décomposition de E en somme directe de sous-espaces :

$$E = \bigoplus_{i=1}^{r} E_i,$$

alors l'espace $\mathrm{End}(E)$ se décompose comme somme directe de sous-espaces $\mathrm{Hom}(E_i, E_j)$: on le voit très bien en formant une base de E à partir de bases des E_i et en considérant un endomorphisme comme une matrice constituée de blocs matriciels indexés par (i,j).

Si les E_i proviennent d'une décomposition de Frobenius de u, le commutant $\mathscr{C}_u$ de u est alors, par biadditivité du « foncteur » Hom, une somme directe :

$$\mathscr{C}_u = \bigoplus_{i,j} \mathrm{Hom}\big(\mathbb{K}[u]x_i, \mathbb{K}[u]x_j\big) \cap \mathscr{C}_u.$$

Soit en effet u dans $\mathscr{C}_u$. Chaque projecteur p_i sur E_i parallèlement à $\bigoplus_{j\neq i} E_j$ appartient à $\mathscr{C}_u$, et l'on a : $u = \sum_{i,j} p_j u p_i$; ainsi, u appartient à la somme directe du membre de droite. L'inclusion inverse est claire.

On peut facilement comprendre l'espace $\bigoplus_{i,j} \mathrm{Hom}\big(\mathbb{K}[u]x_i, \mathbb{K}[u]x_j\big) \cap \mathscr{C}_u$ avec un peu d'abstraction : on a un isomorphisme naturel de $\mathbb{K}[X]/(\mu_{u,x})$ vers $\mathbb{K}[u]\cdot x$, et via cet isomorphisme l'espace $\mathrm{Hom}\big(\mathbb{K}[u]x_i, \mathbb{K}[u]x_j\big) \cap \mathscr{C}_u$ s'identifie à l'espace des morphismes ϕ de $\mathbb{K}[X]/(\mu_{u,x_i})$ vers $\mathbb{K}[X]/(\mu_{u,x_j})$ tels que $\phi(Py) = P\phi(y)$ pour tout P de $\mathbb{K}[X]$.

Pour tout couple (A,B) de polynômes, notons donc $H(A,B)$ l'espace des morphismes ϕ de $\mathbb{K}[X]/(A)$ vers $\mathbb{K}[X]/(B)$ tels que $\phi(Py) = P\phi(y)$ pour tout P de $\mathbb{K}[X]$. On décrit cet espace.

2.4. Proposition. *Soient A et B deux polynômes de $\mathbb{K}[X]$, $D = A \wedge B$ leur pgcd et $B_0 = B/D$. On a les isomorphismes d'espaces vectoriels :*

$$H(A,B) \simeq B_0\mathbb{K}[X]/(B) \simeq \mathbb{K}[X]/(D).$$

Démonstration. On considère le morphisme I qui à ϕ dans $H(A,B)$ associe $\phi(\bar{1})$ dans $\mathbb{K}[X]/(B)$. Alors, I est un isomorphisme de $H(A,B)$ vers $B_0\mathbb{K}[X]/(B)$. Montrons déjà cette première assertion.

1. Le morphisme I est bien (co)défini. Il suffit de montrer que $\phi(\bar{1}) \in B_0\mathbb{K}[X]/(B)$. On a par hypothèses sur ϕ que $0 = \phi(0) = \phi(A\cdot\bar{1}) = A\cdot\phi(\bar{1})$, donc B divise AP, où P est un représentant de $\phi(1) \in \mathbb{K}[X]/(B)$. En posant $A_0 = A/D$, $B_0 = B/D$ (qui sont premiers entre eux) on a

donc B_0 divise A_0P et donc B_0 divise P par le lemme de Gauss. Ainsi, $\phi(\bar{1}) \in B_0\mathbb{K}[X]/(B)$.

2. Le morphisme I est un morphisme d'espaces. Clair.
3. Le morphisme I est injectif : Si $\phi(\bar{1}) = 0$ alors pour tout $\bar{Q}$ de $\mathbb{K}[X]/(A)$, on a $\phi(\bar{Q}) = Q\phi(\bar{1}) = 0$, donc ϕ est le morphisme nul.
4. Le morphisme I est surjectif. Soit $\bar{Q}$ dans $B_0\mathbb{K}[X]/(B)$, alors on va construire ϕ dans $H(A,B)$ tel que $\phi(1) = \bar{Q}$. On a $\bar{Q} = \bar{B}_0\bar{Q}_0$, avec Q_0 dans $\mathbb{K}[X]$. Dans $\mathbb{K}[X]/(B)$, on a $\bar{A}\bar{Q} = \bar{A}\bar{B}_0\bar{Q}_0 = \bar{A}_0\bar{B}\bar{Q}_0 = 0$. Cela prouve que le morphisme $\mathbb{K}[X] \to \mathbb{K}[X]/(B)$, $P \mapsto \overline{QP}$ annule l'idéal (A) et par passage au quotient fournit un morphisme ϕ défini sur $H(A,B)$ tel que $\phi(1) = \bar{Q}$.

Pour finir, on montre que le morphisme $\mathbb{K}[X] \to B_0\mathbb{K}[X]/(B)$, $P \mapsto \overline{B_0P}$ fournit par passage au quotient un isomorphisme $\mathbb{K}[X]/(D) \simeq B_0\mathbb{K}[X]/(B)$ (en exercice). □

2.5. Corollaire. *Soit u un endomorphisme de E et soient $(d_k)_{1\leqslant k\leqslant s}$ les degrés de ses facteurs invariants $(F_k)_{1\leqslant k\leqslant s}$. La dimension de $\mathscr{C}_u$ est :*

$$\dim \mathscr{C}_u = d_1 + 3d_2 + \cdots + (2s-1)d_s = \sum_{i\geqslant 1}(2i-1)d_i.$$

Démonstration. Cela découle directement de la discussion qui précède la proposition : en fixant une décomposition de Frobenius, l'espace $\mathscr{C}_u$ se décompose en somme directe de $\mathrm{Hom}(\mathbb{K}[u]x_i, \mathbb{K}[u]x_j) \cap \mathscr{C}_u$, isomorphes comme espaces à $\mathbb{K}[X]/(F_i \wedge F_j) = \mathbb{K}[X]/(F_k)$, où $k = \min(i,j)$, grâce à la proposition 2.4.

La dimension cherchée est donc :

$$\sum_{i,j} \dim \mathbb{K}[X]/(F_k) = (d_1 + d_2 + d_3 + \cdots + d_s) + (d_2 + d_2 + d_3 + \cdots + d_s) + (d_3 + d_3 + d_3 + \cdots + d_s) + \cdots + (d_s + d_s + d_s + \cdots + d_s),$$

ce qui donne facilement le corollaire. □

Il est permis de préférer à ce résultat sa forme duale, plus agréable. La suite $(d_k)_{1\leqslant k\leqslant s}$ des degrés des facteurs invariants de u est une partition de n.

2.6. Rappel ([H2G2, §III-B]). Une partition de n est une suite décroissante $(d_i)_{i\in\mathbb{N}^*}$ d'entiers dont la somme est n. Son diagramme de Young Y est l'ensemble des couples $(i,j) \in \mathbb{N}^* \times \mathbb{N}^*$ tels que $j \leqslant d_i$. La partition duale de (d_i) est la partition (d_k^*) dont le diagramme de Young est le symétrique de Y par rapport à la diagonale. Quitte à faire un dessin[8], on voit

[8] Cela obligera certains lecteurs à chercher de quoi écrire, voire à descendre du hamac.

([H2G2, lemme III-B.9]) qu'elle est donnée par :

$$\forall k \in \mathbb{N}^*, \quad d_k^* = \big|\{i \in \mathbb{N}^*,\ d_i \geqslant k\}\big|.$$

2.7. Corollaire. *Soit u un endomorphisme de E. Si (d_k^*) est la partition duale de la suite $(d_k)_{1\leqslant k\leqslant s}$ des degrés des facteurs invariants $(F_k)_{1\leqslant k\leqslant s}$ de u, alors la dimension de $\mathscr{C}_u$ est :*

$$\dim \mathscr{C}_u = \sum_k (d_k^*)^2.$$

Démonstration. On veut montrer l'égalité (avec $t = d_1$) :

$$d_1 + 3d_2 + \cdots + (2s-1)d_s = (d_1^*)^2 + (d_2^*)^2 + \cdots + (d_t^*)^2.$$

Montrons-le par récurrence sur le nombre s de parts non nulles de (d_k). Il n'y a rien à vérifier pour la partition vide. On note maintenant $A(d)$ (resp. $B(d)$) le membre de gauche (resp. de droite) de l'égalité, associé à la partition $d = (d_k)_{1\leqslant k\leqslant s}$. Si l'on ajoute une part $d_0 \geqslant d_1$ à la partition, l'examen du diagramme de Young convainc que la nouvelle partition duale est :

$$(d_1^* + 1 \geqslant d_2^* + 1 \geqslant \cdots \geqslant d_s^* + 1 \geqslant \underbrace{1 \geqslant \cdots \geqslant 1}_{d_0 - d_1}).$$

Dans ce cas, $A(d)$ augmente de $d_0 + 2d_1 + 2d_2 + \cdots + 2d_s$, c'est-à-dire de $d_0 + 2\sum_i d_i = d_0 + 2n$. D'autre part, $B(d)$ augmente de $2d_1^* + 1^2 + 2d_2^* + 1^2 + \cdots + 2d_t^* + 1^2 + (d_0 - d_1) \times 1^2$, c'est-à-dire de $2\sum_{i\geqslant 1} d_i^* + t + d_0 - d_1 = 2n + d_0$, car (d_i^*) est une partition de n et $t = d_0$. Cela conclut la récurrence.

Alternativement, on part de l'égalité bien connue : $(d_k^*)^2 = \sum_{i=1}^{d_k^*}(2i-1)$ pour tout k. Par suite, $B(d)$ est une somme des nombres impairs, où pour $i \geqslant 1$, le nombre $2i-1$ intervient autant de fois qu'il y a d'indices k tels que $d_k^* \leqslant i$. Comme (d_i) est la partition duale de (d_k^*), $2i-1$ apparaît d_i fois dans la somme. En formule :

$$\sum_{k\geqslant 1}(d_k^*)^2 = \sum_{k\geqslant 1}\sum_{i\geqslant d_k^*}(2i-1) = \sum_{i\geqslant 1}\sum_{k,\ d_k^*\geqslant i}(2i-1) = \sum_{i\geqslant 1}(2i-1)d_i. \qquad \square$$

On trouve une preuve « en images » de ce résultat dans [58, p. 187-188].

2.8. Exercice. *On suppose que u est un endomorphisme de $\mathbb{K}^n$ tel que $u^2 = 0$ et $\dim\ker(u) = d$. Montrer que $\dim \mathscr{C}_u = (n-d)^2 + d^2$.*

2.9. Corollaire. *La codimension du commutant de l'endomorphisme u est paire.*

Démonstration. Par le corollaire 2.5, la parité de la codimension est :

$$n^2 - \sum_{i\geqslant 1}(2i-1)d_i \equiv n^2 + \sum_{i\geqslant 1} d_i \equiv n^2 + n \equiv 0 \pmod 2. \qquad \square$$

2.10. Remarque. Cette parité n'est pas anodine, car derrière elle se cache une structure de variété symplectique sur les orbites coadjointes, exploitée en théorie de Lie et ses ramifications quantiques. Voir l'exercice VI-B.9 pour plus de précisions.

2.11. Le bicommutant

Nous allons voir que l'étude du bicommutant est paradoxalement beaucoup plus simple. Le bicommutant $\mathscr{C}_u^2$ est par définition l'ensemble des endomorphismes de E qui commutent avec $\mathscr{C}_u$. C'est donc encore une fois une sous-algèbre de $\mathrm{End}_{\mathbb{K}}(E)$, et comme u commute avec son commutant (c'est même une lapalissade), u appartient à son bicommutant. Ainsi : $\mathbb{K}[u] \subset \mathscr{C}_u^2$. On a en fait égalité.

2.12. Théorème. *Le bicommutant $\mathscr{C}_u^2$ de u est l'algèbre $\mathbb{K}[u]$.*

Démonstration. Nous venons de montrer une inclusion ; il reste à montrer l'inclusion inverse. Soit $v \in \mathscr{C}_u^2$. Fixons une décomposition de Frobenius de $E = \bigoplus_{k=1}^{s} \mathbb{K}[u]\cdot x_k$. Comme on l'a vu plus haut, les projecteurs p_k $(1 \leqslant k \leqslant s)$ associés à cette décomposition commutent avec u. Donc, par définition, l'endomorphisme v commute avec tous les p_k. L'endomorphisme v stabilise donc les sous-espaces cycliques $\mathbb{K}[u]\cdot x_k$. Soit donc v_k la restriction de v à $\mathbb{K}[u]\cdot x_k$; on notera u_k l'endomorphisme induit par u sur cet espace. Comme u est dans $\mathscr{C}_u$, l'endomorphisme v commute avec u et donc v_k est dans le commutant de l'espace u_k-cyclique $\mathbb{K}[u]\cdot x_k$. Donc, par la proposition 2.2, v_k est un polynôme Q_k en u_k.

D'après la proposition 2.4 et la discussion qui la précède, il existe pour tout m un (unique) endomorphisme ξ_m de $\mathscr{C}_u$ qui envoie x_1 sur x_m et x_k vers 0 pour tout $k \neq 1$. Plus précisément, si $\phi_m \in \mathrm{Hom}(\mathbb{K}[u]x_1, \mathbb{K}[u]x_m) \cap \mathscr{C}_u$ s'identifie à la projection canonique $\mathbb{K}[X]/(F_1) \to \mathbb{K}[X]/(F_m)$, alors toutes les composantes de ξ_m dans la somme $\bigoplus_{(i,j)} \mathrm{Hom}(\mathbb{K}[u]x_i, \mathbb{K}[u]x_j) \cap \mathscr{C}_u$ sont nulles, à l'exception de ϕ_m.

Comme v commute avec ξ_m, on a :

$$\begin{aligned} v(x_m) &= v\big(\xi_m(x_1)\big) = \xi_m\big(v(x_1)\big) = \xi_m\big(Q_1(u)x_1\big) = Q_1(u)\xi_m(x_1) \\ &= Q_1(u)x_m. \end{aligned}$$

Comme cette égalité est valable pour tout m et comme v commute avec u, il vient : $v = Q_1(u)$ sur $\bigoplus_{k=1}^{s} \mathbb{K}[u]\cdot x_k$, donc sur E. $\square$

2.13. Exemple. En particulier, si u est une homothétie, alors $\mathscr{C}_u = \mathrm{End}(E)$ et l'on retrouve le résultat bien connu que seules les homothéties commutent avec tout $\mathrm{End}(E)$.

3. Désingularisation de Springer du cône nilpotent

Comme il est question de topologie, le corps $\mathbb{K}$ est ici $\mathbb{R}$ ou $\mathbb{C}$. Dans cette partie, on fixe un entier n et l'on note :

$$\mathscr{N} = \big\{N \in \mathscr{M}_n(\mathbb{K}),\ N^n = 0\big\}.$$

La désingularisation de Springer est devenu un outil fondamental dans la théorie de Lie ; nous ne ferons ici qu'effleurer le sujet (le difficile livre [16] semble le point d'entrée le moins inaccessible). Pour donner une motivation, on a vu comment la décomposition de Dunford rend centrales les matrices nilpotentes dans la théorie de la réduction. L'ensemble $\mathscr{N}$ est un cône (si $N \in \mathscr{N}$ et $\lambda \in \mathbb{K}$, alors $\lambda N \in \mathscr{N}$), mais clairement pas un sous-espace vectoriel de l'espace des matrices. En fait, il s'agit même d'une variété algébrique.

Or, on peut se convaincre que tout cône qui n'est pas un sous-espace possède au moins une singularité (on va dire un point non lisse) : le sommet du cône. Selon une méthode très générale qui a fait ses preuves en mathématiques, il est naturel de cherche un objet « lisse » $\mathscr{S}$ qui serait le plus proche possible du cône nilpotent $\mathscr{N}$. C'est ce que nous allons découvrir ici. Nous montrerons deux propriétés censées nous convaincre que $\mathscr{S}$ est bien l'objet convoité.

Le cône nilpotent $\mathscr{N}$ est muni de l'action par conjugaison du groupe $G = \mathrm{GL}_n(\mathbb{K})$. On reprend l'espace topologique $\mathscr{B}$ des drapeaux complets de $\mathbb{K}^n$, muni de l'action naturelle de G par image directe. On notera $F_\bullet^{\mathrm{std}} \in \mathscr{B}$ le drapeau complet standard, constitué des sous-espaces emboîtés $F_k^{\mathrm{std}} = \langle e_1, \dots, e_k\rangle$ engendrés par les k premiers vecteurs de la base canonique $(e_i)_{1\leqslant i\leqslant n}$ (pour $1 \leqslant k \leqslant n$). On sait que l'application orbitale $g \mapsto g \cdot F_\bullet^{\mathrm{std}}$ fournit un homéomorphisme entre G/B et $\mathscr{B}$, où B est le stabilisateur de $F_\bullet^{\mathrm{std}}$, c'est-à-dire le sous-groupe des matrices triangulaires supérieures de G.

Soit $\mathscr{S} = \big\{(N, F_\bullet),\ \forall k \in \{1, \dots, n\},\ N(F_k) \subset F_k\big\} \subset \mathscr{N} \times \mathscr{B}$.

L'ensemble $\mathscr{S}$ est muni de la topologie induite par celle de $\mathscr{N} \times \mathscr{B}$, et il s'agit même d'une variété algébrique (mais ça, c'est une autre histoire). Considérons l'action de G sur $\mathscr{N} \times \mathscr{B}$ définie par : $g \cdot (N, F_\bullet) = (gNg^{-1}, g \cdot F_\bullet)$ pour $g \in G$ et $(N, F_\bullet) \in \mathscr{N} \times \mathscr{B}$. Elle préserve $\mathscr{S}$: si $(N, F_\bullet)$ est dans $\mathscr{S}$, il en est de même de $g \cdot (N, F_\bullet)$.

On va maintenant réaliser $\mathscr{S}$ comme un espace topologique plus classique : le produit fibré $G \times^B \mathfrak{u}$. Pour cela, il faut encore quelques notations.

Soit[9] $\mathfrak{u}$ le sous-espace des matrices triangulaires strictement supérieures et soit $G \times \mathfrak{u}$ le produit direct par G. On vérifie que l'on définit une action à droite de B sur $G \times \mathfrak{u}$ par :

$$(g,u) * b = (gb, b^{-1}ub) \quad (b \in B,\ g \in G,\ u \in \mathfrak{u}).$$

On peut alors définir : $G \times^B \mathfrak{u} = (G \times \mathfrak{u})/B$.

Enfin, l'action de G sur $G \times \mathfrak{u}$ définie par $h \cdot (g,u) = (hg,u)$ $(h,g \in G,$ $u \in \mathfrak{u})$ commute avec l'action de B $\big((h \cdot (g,u)) * b = h \cdot ((g,u) * b)\big)$. On en déduit que G agit sur le quotient $G \times^B \mathfrak{u}$.

3.1. Proposition. *L'application $\varphi : G \times \mathfrak{u} \to \mathscr{S}$, $(g,u) \mapsto (gug^{-1}, g \cdot F_\bullet^{\mathrm{std}})$ définit par passage au quotient un homéomorphisme G-équivariant $\bar{\varphi}$ entre le produit fibré $G \times^B \mathfrak{u}$ et $\mathscr{S}$.*

Démonstration. On vérifie tout d'abord que φ est bien (co)définie puisque l'on a pour tout k l'inclusion : $gug^{-1}\big(g(F_k^{\mathrm{std}})\big) = gu(F_k^{\mathrm{std}}) \subset g(F_k^{\mathrm{std}})$. Ainsi, $(gug^{-1}, g \cdot F_\bullet^{\mathrm{std}})$ appartient à $\mathscr{S}$. De plus, on a : $\varphi\big(h \cdot (g,u)\big) = \varphi(hg,u) = (hgu(hg)^{-1}, hg \cdot F_\bullet^{\mathrm{std}}) = h \cdot (gug^{-1}, g \cdot F_\bullet^{\mathrm{std}}) = h \cdot \varphi(g,u)$ pour $h,g \in G$ et $u \in \mathfrak{u}$, donc φ est G-équivariante.

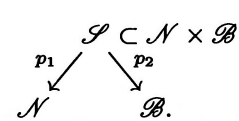
Reste à montrer que l'image réciproque d'un élément $(N, F_\bullet)$ de $\mathscr{S}$ est une B-orbite. Montrons-le tout d'abord dans le cas où $(N, F_\bullet) = (u, F_\bullet^{\mathrm{std}})$ dans $\mathscr{S}$. On veut décrire les couples (g,u') dans $G \times \mathfrak{u}$ tels que $gu'g^{-1} = u$ et $g \cdot F_\bullet^{\mathrm{std}} = F_\bullet^{\mathrm{std}}$. La seconde égalité équivaut à dire que g est dans B, le stabilisateur de $F_\bullet^{\mathrm{std}}$; la première au fait que $u' = g^{-1}ug$. Autrement dit : $\varphi^{-1}\big((u, F_\bullet^{\mathrm{std}})\big) = (\mathrm{Id}, u) * B$.

Passons au cas général. Il existe g tel que $g \cdot F_\bullet^{\mathrm{std}} = F_\bullet$. Posons alors : $u = g^{-1}Nu$, de sorte que l'on a : $(u, F_\bullet^{\mathrm{std}}) = g^{-1} \cdot (N, F_\bullet) \in \mathscr{S}$. Comme u stabilise le drapeau standard, u est triangulaire (strictement) supérieure, c'est-à-dire que $u \in \mathfrak{u}$. Ainsi :

$$\begin{aligned}\varphi^{-1}\big((N, F_\bullet)\big) &= \varphi^{-1}\big(g \cdot (u, F_\bullet^{\mathrm{std}})\big) = g \cdot \varphi^{-1}\big((u, F_\bullet^{\mathrm{std}})\big) \\ &= g \cdot \big((\mathrm{Id}, u) * B\big) = \big((g \cdot (u, F_\bullet^{\mathrm{std}})\big) * B = (N, F_\bullet) * B. \quad \square\end{aligned}$$

On définit les projections naturelles :

$$\begin{cases} p_1 : \mathscr{S} \to \mathscr{N}, & (N, F_\bullet) \mapsto N \\ p_2 : \mathscr{S} \to \mathscr{B}, & (N, F_\bullet) \mapsto F_\bullet \end{cases}$$



[9] On reconnaît l'algèbre de Lie du sous-groupe U des éléments unipotents de B.

3.2. Proposition. *Les projections p_1, p_2 sont des G-morphismes. De plus :*

(i) *pour tout N de $\mathscr{N}$, la fibre $p_1^{-1}(N)$ est compacte ;*

(ii) *la fibre de l'origine 0 de $\mathscr{N}$ est : $p_1^{-1}(0) = \{0\} \times \mathscr{B}$;*

(iii) *pour N dans l'orbite dense de $\mathscr{N}$, la fibre $p_1^{-1}(N)$ est un point ;*

(iv) *pour tout $F_\bullet$, la fibre $p_2^{-1}(F_\bullet)$ est un espace vectoriel de dimension constante $n(n-1)/2$.*

Démonstration. Il est immédiat que p_1 et p_2 commutent avec l'action de G.

(i) On a $p_1^{-1}(N) = \{N\} \times \mathscr{G}$, où $\mathscr{G}$ est l'ensemble des drapeaux $F_\bullet$ tels que $N(F_k) \subset F_k$ pour tout k. Il suffit de montrer que $\mathscr{G}$ est compact. Comme la variété des drapeaux $\mathscr{B}$ est compacte, il reste à voir que $\mathscr{G}$ est fermé. En notant π la projection $G \to G/B \simeq \mathscr{B}$, cela revient à montrer que $\pi^{-1}(\mathscr{G})$ est fermé. Or, $\pi^{-1}(\mathscr{G})$ est l'ensemble des g tels que $N(gF_0^k) \subset gF_0^k$ pour tout k, ce qui s'écrit aussi : $g^{-1}Ng \in \mathfrak{u}$. Cette condition s'exprime par l'annulation de certains coefficients de $g^{-1}Ng$, qui sont des fonctions continues de g. C'est donc bien une condition fermée.

(ii) L'assertion vient de ce que l'application nulle préserve tous les drapeaux.

(iii) On rappelle que, par [H2G2, corollaire III-2.7.3], l'action par conjugaison de G sur $\mathscr{N}$ a une orbite dense, celle du bloc de Jordan

$$J_n = \begin{pmatrix} 0 & 1 & 0 & 0 \\ \vdots & \ddots & \ddots & 0 \\ \vdots & & \ddots & 1 \\ 0 & \cdots & \cdots & 0 \end{pmatrix}.$$

Comme $J_n^k(E) = F_{n-k}^{\mathrm{std}}$, le seul drapeau que J_n préserve est le drapeau standard $F_\bullet^{\mathrm{std}}$. Ainsi, $p_1^{-1}(J_n)$ est réduit à un point et l'assertion s'en déduit par principe de translation.

(iv) On a vu précédemment la relation : $p_2^{-1}(F_\bullet^{\mathrm{std}}) = \mathfrak{u}$. L'assertion s'en déduit encore par translation. □

Reformulons les résultats pour voir en quoi $p_1 : \mathscr{S} \to \mathscr{N}$ mérite le nom de désingularisation. D'après la proposition 3.1, la variété $\mathscr{S}$ est « lisse ». La proposition 3.2 (iii) montre que sur une partie dense de $\mathscr{N}$, qui est une G-orbite et donc n'a pas de singularité, p_1 est bijective ; cela exprime une certaine minimalité de $\mathscr{S}$. En revanche, l'assertion (ii) exprime que la fibre au-dessus de 0, qui est le point le plus singulier du cône nilpotent, est la plus grande possible puisque c'est $\mathscr{B}$ tout entier.

Inversement, on peut voir le cône nilpotent comme la G-variété (lisse) $\mathscr{S}$ que l'on aurait « froissée » par endroits. Plus on a froissé en un point

de $\mathcal{N}$, plus grande est la dimension de la fibre en ce point. Si un point est dans l'orbite dense, cette dimension est nulle et il n'y a pas eu froissement en ce point. En revanche, si l'on est au sommet du cône, c'est-à-dire la matrice nulle, le froissement est maximal — voir la figure XI-8.1 p. 529 pour une image dans le cas $n = 2$. Les auteurs sont sincèrement désolés pour ces images simplistes de la désingularisation et espèrent n'avoir froissé personne.

A. Plaidoyer pour les modules

Étonnant, non ?

Pierre Desproges, *La minute nécessaire de M. Cyclopède*, 1982.

Il est classique de ramener l'étude des espaces vectoriels munis d'un endomorphisme à la théorie des modules sur l'anneau des polynômes $\mathbb{K}[X]$. On rappelle brièvement le dictionnaire et l'on donne une preuve non standard du théorème de Cayley-Hamilton. Cette application de la *structure* même devrait motiver l'introduction d'algèbres dans les contextes des représentations des carquois (chapitre III) et des groupes (annexe X-D).

On peut aller bien plus loin : du fait que $\mathbb{K}[X]$ est principal et même euclidien, les théorèmes de structure sur les $\mathbb{K}[X]$-modules deviennent des théorèmes de réduction. Le théorème des diviseurs élémentaires donne la réduction de Frobenius et de la décomposition primaire découle la réduction de Jordan. On peut poursuivre en donnant un algorithme dérivé du pivot de Gauss pour trouver les facteurs invariants d'une matrice.

A.1. Modules sur un anneau

Dans plusieurs passages du livre, nous parlons de *A-modules*, où A désigne un anneau unitaire. Il s'agit d'une notion souvent connue en M1, que nous rappelons rapidement ici. Pour plus de détails, voir par exemple [65]. On dit souvent pour faire bref — et faux — qu'un module est un « espace vectoriel sur un anneau ». Remplacez dans les axiomes classiques d'espace vectoriel le corps de base $\mathbb{K}$ par un anneau A et vous obtiendrez naturellement la définition d'un A-module. On obtient aussi de façon analogue les notions de sous-module, de morphismes de A-modules, de produit de A-modules...

Plus précisément, un *A-module* M est un groupe abélien, noté additivement en général, muni d'un morphisme d'anneaux unitaires $\alpha : A \to \mathrm{End}(M)$, où $\mathrm{End}(M) = \mathrm{End}_{\mathbb{Z}}(M)$ désigne l'anneau des morphismes du groupe M dans lui-même. En notant $\alpha(a)(m) = a \cdot m$ (ou simplement am) pour tous $a \in A$ et $m \in M$, on retrouve bien les axiomes (avec a, b dans A et m, n dans M) :

$$a\cdot(m+n)=a\cdot m+a\cdot n,\ (a+b)\cdot m=a\cdot m+b\cdot m,\ a\cdot(b\cdot m)=(ab)\cdot m,\ 1\cdot m=m.$$

Un *sous-module* est alors un sous-groupe de M stable par $\alpha(A)$.

Un *morphisme* entre deux A-modules M et N est un morphisme de groupes $\psi : M \to N$ tel que pour tous $a \in A$ et $m \in M$, on a :

$$\psi(a \cdot m) = a \cdot \psi(m).$$

Quelques mots supplémentaires pour référence ultérieure. On dit qu'un A-module M est *irréductible* ou *simple* s'il n'est pas réduit à $\{0\}$ et si ses seuls sous-modules sont $\{0\}$ et M.

Étant donnés un A-module M et un sous-module M' de M, le *module-quotient* M/M' est défini naturellement comme suit. En tant que groupe, c'est le quotient habituel M/M'. Pour a dans A et $\mathbf{m}$ un élément du quotient, on choisit un représentant m de $\mathbf{m}$ dans M, de sorte que $\mathbf{m} = m+M'$; comme M' est un sous-module, la classe de $a \cdot m$ ne dépend que de $\mathbf{m}$ et pas du choix de m : on définit $a \cdot \mathbf{m}$ comme cette classe. Les axiomes de module se vérifient facilement.

A.2. Remarque (Existence de bases ?). Apparemment rien de nouveau par rapport aux espaces vectoriels, mais un drame profond se noue du côté des A-modules : le théorème de la base incomplète n'y a plus cours. Entre autres, il n'existe en général pas de base et même parfois pas de partie libre ! Toute la théorie de la dimension s'effondre lamentablement. On l'aura compris : un A-module est bien un « espace vectoriel sur un anneau », mais la théorie changeant de façon dramatique, il est plus prudent de modifier la terminologie.

A.3. Remarque (Somme directe et indécomposabilité). Étant donnés deux A-modules M' et M'', on voit bien comment construire leur *somme directe* : comme groupe, c'est la somme directe[10] $M' \oplus M''$; l'action d'un élément a de A sur un élément (m', m'') de $M \oplus M''$ est simplement : $a \cdot (m', m'') = (a \cdot m', a \cdot m'')$. On peut alors parler de supplémentaires.

Dans le même esprit que la remarque précédente, il est bien connu que le théorème de la base incomplète entraîne (avec l'axiome du choix) l'existence de supplémentaires. Cette propriété est fausse en général pour les modules : un sous-module M' d'un module M ne possède pas nécessairement de supplémentaire (prendre $A = \mathbb{Z}$, $M = \mathbb{Z}$, $M' = 2\mathbb{Z}$; d'autres exemples sont proposés ci-dessous).

Cela justifie la définition suivante : un A-module M est *indécomposable* s'il n'est pas réduit à $\{0\}$ et s'il est impossible d'en trouver deux sous-modules M' et M'' tels que $M \simeq M' \oplus M''$.

[10] Comme il n'y a que deux facteurs, la somme directe s'identifie au produit $M' \times M''$.

A.4. Modules sur une algèbre

Soit A une algèbre unitaire sur un corps $\mathbb{K}$. Alors, comme $\mathbb{K}$ est un sous-anneau de A, tout A-module est muni d'une structure naturelle de $\mathbb{K}$-espace vectoriel et α est un morphisme de $\mathbb{K}$-algèbres de A vers la $\mathbb{K}$-algèbre $\mathrm{End}_{\mathbb{K}}(M)$ des endomorphismes de l'espace vectoriel M.

A.5. Exercice. *Soit A une algèbre sur un corps $\mathbb{K}$ et soit M un A-module qui est de dimension finie sur $\mathbb{K}$. On considère un sous-espace vectoriel M' de M et M'' un supplémentaire de M' dans M — en général, ce ne sont pas des sous-modules. On construit une base de M en recollant une base de M' et une de M''.*

1. *Montrer que M' est un sous-module si et seulement si pour tout a de A, la matrice de l'application $a_M : M \to M$, $m \mapsto a \cdot m$ dans cette base est triangulaire par blocs,* i.e. *de la forme* $\mathrm{mat}(a_M) = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$.

   On suppose désormais que M' est un sous-module de M.
2. *Montrer qu'avec les notations ci-dessus, α est la matrice de l'application $a_{M'} : M' \to M'$, $m \mapsto a \cdot m$ et que δ est celle de l'application analogue $a_{M/M'} : M/M' \to M/M'$, exprimée dans la base image de la base de M'' par la projection canonique $M \to M/M'$.*
3. *Étendre ce qui précède à la dimension quelconque en donnant un sens à l'écriture matricielle suivante de a_M pour tout a de A :*

$$\begin{pmatrix} a_{M'} & c_{M',M''}(a) \\ 0 & a_{M/M'} \end{pmatrix}, \quad \text{avec } c_{M',M''}(a) \in \mathrm{Hom}_{\mathbb{K}}(M'', M').$$

   On identifie M'' et M/M' comme espaces vectoriels. Vérifier que cette écriture est compatible avec la composition : la matrice associée à $(ab)_M$ est bien le produit des matrices associées à a_M et b_M (où $a, b \in A$).

A.6. Dictionnaire entre endomorphismes et $\mathbb{K}[X]$-modules

On fixe un corps $\mathbb{K}$. Étant donnés un espace vectoriel E et un endomorphisme u de E, on définit un $\mathbb{K}[X]$-*module* M_E de la façon suivante : comme groupe additif, M_E est E ; l'action d'un polynôme $P = \sum_{i=0}^{d} a_i X^i$ de $\mathbb{K}[X]$ sur un vecteur v de M_E est définie[11] par : $P \cdot v = P(u)(v) = \sum_{i=0}^{d} a_i u^i(v)$. On vérifie sans peine que cela fait de M_E un $\mathbb{K}[X]$-module.

Remarque. Le lecteur vigilant n'aura pas manqué de noter, lors de la vérification des axiomes qui font de M_E un $\mathbb{K}[X]$-module, que ceux-ci sont équivalents à la propriété bien connue que l'évaluation en u fournit un morphisme de $\mathbb{K}$-algèbre unitaire entre $\mathbb{K}[X]$ et $\mathrm{End}_{\mathbb{K}}(E)$.

[11] Bien sûr, on définit les puissances par : $u^0 = \mathrm{Id}_E$ et $u^{i+1} = u \circ u^i$ pour tout entier i.

Inversement, si M est un $\mathbb{K}[X]$-module, on pose $E = E_M$; on fait de E_M un espace vectoriel en restreignant le produit $\mathbb{K}[X] \times M \to E_M$ aux polynômes constants, d'où un produit $\mathbb{K} \times E_M \to E_M$; on munit E_M de l'endomorphisme $u : E_M \to E_M$, $v \mapsto X \cdot v$ (comme $\mathbb{K}[X]$ est une algèbre, u est bien linéaire ; on a, avec les notations ci-dessus : $u = X_M$).

Bien sûr, ces deux correspondances sont réciproques l'une de l'autre. Cela provient du fait que $P(X)$ agit comme $P(u)$ pour tout polynôme $P(X)$.

Traduisons les notions standard associées aux modules. Un morphisme de $\mathbb{K}[X]$-modules est une application $\psi : M \to M'$ qui commute avec l'action de X. Si u et u' sont les endomorphismes correspondant à la multiplication par X respectivement dans M et dans M', la condition sur ψ devient : $u' \circ \psi = \psi \circ u$; on dit que ψ *entrelace* u et u'.

A.7. Proposition. *Avec les notations ci-dessus, les endomorphismes u et u' de l'espace E sont semblables si et seulement si les $\mathbb{K}[X]$-modules M et M' sont isomorphes.*

Démonstration. Supposons qu'il existe un isomorphisme ψ de M vers M'. Comme ψ est en particulier un endomorphisme de l'espace E, on voit que $u' = \psi \circ u \circ \psi^{-1}$ est semblable à u.

Réciproquement, si $u' = \psi \circ u \circ \psi^{-1}$, avec $\psi \in \mathrm{GL}(E)$. On peut définir ψ de M vers M'. Alors, il est immédiat que pour tout x dans M, on a : $\psi(X \cdot x) = \psi\big(u(x)\big) = u'\big(\psi(x)\big) = X \cdot \psi(x)$. Et donc, ψ établit bien un isomorphisme entre les $\mathbb{K}[X]$-modules M et M'. □

Un *sous-$\mathbb{K}[X]$-module* est un sous-groupe additif stable par produit par un polynôme : considérant les polynômes constants, on voit que c'est en particulier un sous-espace vectoriel ; prenant le polynôme X, on voit qu'il est stable par l'endomorphisme correspondant. Inversement, un sous-espace stable par l'endomorphisme est bien un sous-module.

Si l'on quotiente un espace E par un sous-espace F stable par u, on peut définir un endomorphisme $\bar{u}$ sur le quotient : en notant $v + F$ la classe modulo F d'un vecteur v de E, on pose : $\bar{u}(v + F) = u(v) + F$. Cela ne dépend pas du choix de v dans $v + F$ puisque si $v - v' \in F$, on a : $u(v) - u(v') \in u(F) \subset F$. Le couple $(E/F, \bar{u})$ correspond au $\mathbb{K}[X]$-*module-quotient* E/F.

Ce petit dictionnaire est résumé dans le tableau suivant.

e.v. muni d'un endomorphisme	$\mathbb{K}[X]$-module
(E,ϕ)	$M=E$
$u(v)=X\cdot v$	$P(X)\cdot v=P(u)(v)$
morphisme $\psi : E\to E'$ qui entrelace u et u'	morphisme de $\mathbb{K}[X]$-module
sous-espace stable par u	sous-module
quotient par un sous-espace stable	module-quotient

Tout ce qui précède établit une équivalence de catégories (si, si !) entre espaces vectoriels munis d'un endomorphisme et modules sur $\mathbb{K}[X]$.

A.8. Exemple (Matrice compagnon). Soit $P=X^s+b_{s-1}X^{s-1}+\cdots+b_0$ un polynôme unitaire de degré $s\geqslant 1$. La *matrice compagnon* de P est

$$C(P)=\begin{pmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -b_{s-2} \\ 0 & \cdots & 0 & 1 & -b_{s-1} \end{pmatrix}.$$

Elle est naturellement attachée à P de la façon suivante : l'idéal (P) engendré par P est un sous-$\mathbb{K}[X]$-module de $\mathbb{K}[X]$; le quotient $M=\mathbb{K}[X]/(P)$ est un $\mathbb{K}[X]$-module de dimension s, dont une base naturelle est l'image de la famille libre $(1,X,\ldots,X^{s-1})$ par la projection naturelle ; alors, $C(P)$ est la matrice de l'endomorphisme $u=X_M$ dans cette base (vérifier !).

À titre d'exercice, on peut démontrer que M est irréductible (comme module) si et seulement si P est irréductible (comme polynôme) ; semi-simple si et seulement si les facteurs irréductibles de P ont pour multiplicité 1 ; indécomposable si et seulement si P n'a qu'un seul facteur irréductible.

A.9. Remarque. Ce qui précède permet, entre autres, d'utiliser le lemme chinois dans les problèmes de réduction des endomorphismes. Par exemple, soit u un endomorphisme dont la matrice dans une base est diagonale par blocs, les blocs diagonaux étant les matrices compagnons $C(P)$ et $C(Q)$ pour P et Q, polynômes premiers entre eux de $\mathbb{K}[X]$. Alors, d'après [H2G2, proposition III-5.5], le module associé M est isomorphe à $\mathbb{K}[X]/(P)\oplus\mathbb{K}[X]/(Q)\simeq\mathbb{K}[X]/(PQ)$, ce qui permet de voir que u admet une matrice égale à $C(PQ)$ dans une base convenable.

Voici maintenant une application non triviale de cette structure de $\mathbb{K}[X]$-module, qui est en soi un plaidoyer pour l'étude des endomorphismes via les $\mathbb{K}[X]$-modules.

A.10. Théorème (Cayley-Hamilton). *Soit A une matrice carrée à coefficients dans un corps $\mathbb{K}$ et soit χ_A son polynôme caractéristique. Alors, on a :*

$$\chi_A(A) = 0.$$

Démonstration. On note n la taille de la matrice A. Soit $M = \mathbb{K}^n$ le $\mathbb{K}[X]$-module sur lequel X opère par la matrice A. On introduit alors l'anneau de matrices $R = \mathscr{M}_n(\mathbb{K}[X])$ et l'on fait de M^n un R-module de façon naturelle : si $B = (b_{ij})_{1\leqslant i,j\leqslant n}$ est un élément de R et $m = (m_i)_{1\leqslant i\leqslant n}$ appartient à M, on pose : $Bm = \left(\sum_{j=1}^n b_{ij}\cdot m_j\right)_{1\leqslant i\leqslant n}$.

Soit $(e_i)_{1\leqslant i\leqslant n}$ la base canonique de l'espace vectoriel M. On a donc, par définition :

$$\forall j \in \{1,\dots,n\},\quad X\cdot e_j = \sum_{i=1}^n a_{ij}e_i.$$

Autrement dit, en posant $B = X\mathrm{I}_n - A \in \mathscr{M}_n(\mathbb{K}[X])$ et $\mathbf{e} = (e_1,\dots,e_n) \in M^n$, on a : $B\mathbf{e} = 0 \in M^n$. Soit C la transposée de la comatrice de B, calculée dans $R = \mathscr{M}_n(\mathbb{K}[X])$. On a par la règle de Cramer : $CB = \det(B)\mathrm{I}_n$, où $\det(B) = \det(X\mathrm{I}_n - A)$ est le polynôme caractéristique χ_A de A. Or, par associativité généralisée, on a :

$$\det(B)\mathbf{e} = \det(B)\mathrm{I}_n\mathbf{e} = CB\mathbf{e} = C0 = 0,$$

et $\det(B)$ agit sur M^n comme la multiplication par $\chi_A(A)$. Il vient donc : $\chi_A(A)e_j = 0$ pour tout j. Comme (e_j) est une base de M, il vient : $\chi_A(A) = 0 \in \mathscr{M}_n(\mathbb{K})$. □

Bien sûr, la théorie des modules donne beaucoup plus que le théorème de Cayley-Hamilton. Du fait que l'anneau $\mathbb{K}[X]$ est principal, et même euclidien, la théorie de la réduction des endomorphismes est strictement parallèle à celle des groupes abéliens, où l'on trouve des analogues de la réduction de Jordan ou de Frobenius. Le livre [39] de Daniel Guin suit ce point de vue, voir aussi [58, §C.11.70].

A.11. Dictionnaire (suite)

Le dictionnaire du §A.6 se prolonge avec les notions du chapitre.

e.v. muni d'un endomorphisme	$\mathbb{K}[X]$-module
commutant de u	endomorphismes de module
espace u-cyclique	module cyclique (monogène)
endomorphisme simple	module simple
endomorphisme semi-simple	module semi-simple

Afin d'illustrer ce dernier tableau, remarquons que si u est un endomorphisme cyclique de E, et si l'on note x un vecteur tel que $E = \mathbb{K}[u] \cdot x$, alors l'application $P \mapsto P(u) \cdot x$ définit un morphisme (d'espaces) surjectif de $\mathbb{K}[X]$ sur E. On voit que si l'on munit $\mathbb{K}[X]$ de sa structure naturelle de $\mathbb{K}[X]$-module par multiplication à gauche, alors, on obtient ainsi un morphisme de $\mathbb{K}[X]$-modules de $\mathbb{K}[X]$ sur M. Par passage au quotient, on obtient un isomorphisme de $\mathbb{K}[X]$-modules $\mathbb{K}[X]/(\mu_u) \simeq M$, où μ_u désigne le polynôme minimal de u, qui est également dans ce cas le polynôme minimal P tel que $P(u) \cdot x = 0$.

Ainsi, le théorème 1.1 de décomposition de Frobenius se traduit directement en langage de $\mathbb{K}[X]$-modules.

A.12. Théorème. *Soit u un endomorphisme d'un espace E sur $\mathbb{K}$ et soit M le $\mathbb{K}[X]$-module associé. Alors, il existe un unique entier naturel s et une unique famille de polynômes unitaires non constants $(F_1, \dots, F_s)$ de $\mathbb{K}[X]$ tels que :*

(i) $F_s \mid F_{s-1} \mid \cdots \mid F_1$;

(ii) $M \simeq \bigoplus_{k=1}^{s} \mathbb{K}[X]/(F_k)$, *comme $\mathbb{K}[X]$-modules.*

On peut aussi apprécier une version de la décomposition de Frobenius sous forme de suites exactes de $\mathbb{K}[X]$-modules. Soit donc u un endomorphisme d'un espace E sur un corps $\mathbb{K}$, et soit M le $\mathbb{K}[X]$-module associé. Soit $(F_1, \dots, F_s)$ la famille d'invariants de similitude de u. On considère la décomposition de Frobenius $M = \bigoplus_{k=1}^{s} \mathbb{K}[X]x_i$, où on a fixé un choix d'éléments x_i de M. Soit $\phi : \mathbb{K}[X]^s \to M$ le morphisme de $\mathbb{K}[X]$-modules donné par $\phi(P_1, \dots, P_s) = \sum_i P_i \cdot x_i$. La décomposition de M en sommes directes donne donc que ϕ est surjectif et que son noyau est $\{(F_i P_i)_{1 \leqslant i \leqslant s},\ P_i \in \mathbb{K}[X]\}$. On peut donc définir le morphisme $\psi : \mathbb{K}[X]^s \to \mathbb{K}[X]^s$ par $\psi(P_1, \dots, P_s) = (F_1 P_1, \dots, F_s P_s)$.

A.13. Corollaire. *Avec les notations ci-dessus, on a la suite exacte de $\mathbb{K}[X]$-modules :*

$$0 \longrightarrow \mathbb{K}[X]^s \xrightarrow{\psi} \mathbb{K}[X]^s \xrightarrow{\phi} M \longrightarrow 0.$$

Interprétons cette suite exacte de la façon suivante : on peut présenter le $\mathbb{K}[X]$-module (non libre) par deux $\mathbb{K}[X]$-modules libres. Cela ressemble sur beaucoup d'aspects à la présentation des groupes par générateurs et relations introduite en I-B. On trouvera l'utilité de cette démarche au moment d'une tentative de classification des sous-espaces u-stables de E, c'est-à-dire des sous-$\mathbb{K}[X]$-modules de M, voir exercice B.10.

Voici pour finir un théorème bien connu (voir par exemple [74, §6.3]) qui permet de déterminer si deux matrices sont semblables à l'aide d'un algorithme de type pivot de Gauss sur l'anneau euclidien $\mathbb{K}[X]$.

On dit que deux matrices A et B de $\mathscr{M}_n(\mathbb{K}[X])$ sont équivalentes sur $\mathscr{M}_n(\mathbb{K}[X])$ s'il existe deux matrices P et Q de $\mathscr{M}_n(\mathbb{K}[X])$, inversibles dans $\mathscr{M}_n(\mathbb{K}[X])$, telles que $B = PAQ$. On admettra le théorème des facteurs invariants qui dit que, comme $\mathbb{K}[X]$ est euclidien[12], il existe, pour tout A de $\mathscr{M}_n(\mathbb{K}[X])$, un unique $0 \leqslant r \leqslant n$ et une unique suite de polynômes unitaires $P_1, \dots, P_r$ de $\mathbb{K}[X]$ tels que P_{i+1} divise P_i dans $\mathbb{K}[X]$ pour tout i, $1 \leqslant i \leqslant r-1$, et tels que A soit équivalente sur $\mathscr{M}_n(\mathbb{K}[X])$ à la matrice diagonale $\operatorname{diag}(P_1, \dots, P_r, 1, \dots, 1)$. Ces éléments sont appelés *facteurs invariants* de A. Ainsi, A et B sont équivalentes sur $\mathscr{M}_n(\mathbb{K}[X])$ si et seulement si elles ont mêmes facteurs invariants.

A.14. Théorème. *Deux matrices A et B de $\mathscr{M}_n(\mathbb{K})$ sont semblables si et seulement si $X\mathrm{I}_n - A$ et $X\mathrm{I}_n - B$ sont équivalentes dans $\mathscr{M}_n\big(\mathbb{K}[X]\big)$.*

Démonstration. Si A et B sont semblables, disons $B = PAP^{-1}$, alors $X\mathrm{I}_n - B = P(X\mathrm{I}_n - A)P^{-1}$, et donc $X\mathrm{I}_n - A$ et $X\mathrm{I}_n - B$ sont également semblables et donc équivalentes.

Réciproquement, supposons que $X\mathrm{I}_n - A$ et $X\mathrm{I}_n - B$ sont équivalentes dans $\mathscr{M}_n\big(\mathbb{K}[X]\big)$. Par [H2G2, corollaire III-5.10], il suffit de montrer que les facteurs invariants de $X\mathrm{I}_n - A$ dans $\mathscr{M}_n(\mathbb{K}[X])$ sont exactement les facteurs invariants de similitude de A. Grâce à la décomposition de Frobenius, [H2G2, corollaire III-5.9], on se ramène à la *matrice compagnon* $C(P)$ du polynôme P de degré s définie ci-dessus.

Montrons donc que la matrice $X\mathrm{I}_s - C(P)$ est équivalente dans $\mathscr{M}_s(\mathbb{K}[X])$ à la matrice diagonale $\operatorname{diag}(P, 1, \dots, 1)$. Cela implique la réciproque : en effet, si $F_1 \mid F_2 \mid \cdots \mid F_k$ sont les polynômes de la décomposition de Frobenius de A, on aura, après permutation dans la diagonale, que $X\mathrm{I}_s - C(P)$ est équivalente à $\operatorname{diag}(F_1, \dots, F_k, 1, \dots, 1)$. Par l'unicité des facteurs invariants (rappelée plus haut), les matrices B et A auront même décomposition de Frobenius, et seront donc semblables par [H2G2, corollaire III-5.10].

On vérifie sans trop de mal que l'on obtient, par les transformations élémentaires suivantes sur les lignes (L_i) et les colonnes (C_j) :

$$L_1/L_1 + \sum_{i=2}^{s} X^{i-1} L_i, \;\; C_2/C_2 + XC_1, \;\; \dots, \;\; C_s/C_s + XC_{s-1},$$

[12] On le montre plus généralement dans pour un anneau principal, mais le cas euclidien permet d'obtenir un algorithme constructif.

opérées successivement, que la matrice $X\mathrm{I}_s - C(P)$ est équivalente à

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & P \\ -1 & 0 & \cdots & 0 & 0 & b_1 \\ 0 & -1 & & 0 & 0 & b_2 \\ \vdots & 0 & & & \vdots & \vdots \\ \vdots & \vdots & \ddots & -1 & 0 & b_{s-2} \\ 0 & 0 & \cdots & 0 & -1 & b_{s-1} \end{pmatrix}.$$

Puis, $C_s/C_s + \sum_{i=1}^{s-1} b_i C_i$ donne $\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & P \\ -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & & 0 & 0 & 0 \\ \vdots & 0 & & & \vdots & \vdots \\ \vdots & \vdots & \ddots & -1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & -1 & 0 \end{pmatrix}$.

Après permutation cyclique des colonnes (donc multiplication à droite par une matrice de permutation), et multiplication par la matrice diagonale $\mathrm{diag}(1, -1, \ldots, -1)$, on obtient bien la matrice voulue. □

La preuve contenait un énoncé notable.

A.15. Corollaire. *Les invariants de similitude*[13] *de la matrice A sont les facteurs invariants de la matrice $X\mathrm{I}_n - A$.*

A.16. Remarque. Ce théorème fournit un algorithme long, mais sûr, pour calculer en pratique les polynômes invariants d'une matrice A. Il suffit pour cela de trouver une matrice diagonale équivalente à $X\mathrm{I}_n - A$. En effet, une matrice diagonale satisfaisant à la condition supplémentaire de divisibilité des polynômes P_i s'obtient par le lemme chinois, en utilisant la remarque A.9.

On voit alors qu'il suffit de faire une méthode de type « pivot de Gauss » afin d'obtenir une matrice diagonale par équivalence. Sauf que les matrices doivent rester à coefficients dans l'anneau $\mathbb{K}[X]$; et c'est là qu'il est nécessaire d'effectuer une variante de l'algorithme de Gauss où la division euclidienne intervient. Pour donner une idée de l'algorithme « euclidianisé », on remarque que la division euclidienne de P par Q donnée par $P = QS + R$,

[13] Rappelons que ce sont des polynômes.

s'interprète à l'aide de matrices de transvections par

$$\begin{pmatrix} 1 & 0 \\ -S & 1 \end{pmatrix}\begin{pmatrix} Q \\ P \end{pmatrix} = \begin{pmatrix} Q \\ R \end{pmatrix} \quad , \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} Q \\ R \end{pmatrix} = \begin{pmatrix} R \\ Q \end{pmatrix}.$$

Cela permet d'interpréter par la suite l'algorithme d'Euclide à l'aide de multiplications par des matrices de transvection et de permutation. On trouve donc, après une suite de telles opérations, une matrice inversible $T \in \mathscr{M}_2(\mathbb{K}[X])$ telle que $T\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} D \\ 0 \end{pmatrix}$, où D est le pgcd de P et Q. On peut donc annuler ainsi la première colonne (à l'exception du coefficient $(1,1)$) de la matrice A, et idem pour la première ligne par transposition.

La suite est laissée à l'imagination débridée du lecteur, qui pourra, faute d'inspiration, se référer à [70].

B. Exercices du chapitre II

Invariants de similitude

B.1. Exercice (Invariants de similitude d'une matrice de permutation)

1. *Montrer que si le polynôme minimal de A est le produit d'irréductibles P_i distincts et si le polynôme caractéristique s'écrit $\chi_A = \prod_i P_i^{\alpha_i}$, alors les invariants de similitude de A sont de la forme $F_k = \prod_{\alpha_i \geqslant k} P_i$.*

   Le premier invariant de similitude F_1 est le polynôme minimal. L'assertion est alors directement impliquée par le fait que les invariants de similitude se divisent successivement et que leur produit est égal au polynôme caractéristique. On peut transcrire cela en termes de tableaux de Young : pour chaque i, le tableau associé à P_i possède une seule ligne et α_i colonnes.

2. *En déduire les invariants de similitude d'une matrice de permutation en fonction de ses cycles.*

   L'ordre m de la permutation est le ppcm des ordres c_i des cycles de sa décomposition. Le polynôme minimal de la matrice est $X^m - 1$ et son polynôme caractéristique $\prod_i (X^{c_i} - 1)$.

B.2. Exercice (Jordan et Frobenius)

Montrer que si un endomorphisme est nilpotent, alors sa matrice dans une base adaptée à la décomposition de Frobenius est une matrice par blocs de Jordan.

Endomorphismes cycliques

B.3. Exercice (Endomorphismes cycliques diagonalisables)

Montrer qu'un endomorphisme complexe cyclique est diagonalisable si et seulement si son polynôme caractéristique n'a que des racines simples.

Pour un endomorphisme cyclique, le polynôme caractéristique et le polynôme minimal coïncident.

B.4. Exercice (Espace cyclique pour une famille d'endomorphismes)

Soit $(A_1, \ldots, A_k)$ une famille finie de matrices qui commutent deux à deux dans $\mathscr{M}_n(\mathbb{C})$. On suppose qu'il existe un vecteur v tel que :

si F est un sous-espace de $\mathbb{C}^n$ contenant v et stable par tous les A_i, alors : $F = \mathbb{C}^n$.

On se propose de montrer que la sous-algèbre des matrices commutant avec tous les A_i est de dimension n et qu'il s'agit de la sous-algèbre $\mathscr{A}$ de $\mathrm{End}(\mathbb{C}^n)$ engendrée par les A_i.

1. *Montrer que tout vecteur w de $\mathbb{C}^n$ s'écrit $w_Q = Q(A_1, \dots, A_k) \cdot v$ pour un polynôme Q de $\mathbb{C}[X_1, \dots, X_k]$.*
   Noter d'abord que $Q(A_1, \dots, A_k)$ fait sens puisque les A_i commutent. Le reste résulte de la définition de v.
2. *Montrer qu'il existe une base de $\mathbb{C}^n$ qui peut s'écrire sous la forme $(w_{Q_i})_i$ pour une famille de polynômes Q_i, $1 \leqslant i \leqslant n$. En déduire que la sous-algèbre des matrices commutant avec tous les A_i est égal à $\mathscr{A}$.*
   On pourra s'inspirer de la preuve de la proposition 2.2.
3. *Soit φ l'application qui, à un polynôme P de $\mathbb{C}[X_1, \dots, X_k]$, associe $\varphi(P) = P(A_1, \dots, A_k) \cdot v$ dans $\mathbb{C}^n$. Montrer qu'il s'agit d'une application linéaire surjective et que son noyau est l'idéal I des polynômes P tels que $P(A_1, \dots, A_k)$ est l'endomorphisme nul.*
4. *Montrer que $\mathbb{C}[X_1, \dots, X_k]/I$ est isomorphe à l'algèbre $\mathscr{A}$ et conclure.*

Sous-espaces stables et semi-simplicité

B.5. Exercice. *Soit E un $\mathbb{K}$-espace et u un endomorphisme cyclique de $E = \mathbb{K}[u] \cdot x$, pour un x de E. Soit F un sous-espace u-stable. Montrer qu'il existe un diviseur D du polynôme minimal μ_u de u tel que $F = \mathbb{K}[u] \cdot D(u)(x)$.*

Soit $\pi_u : \mathbb{K}[X] \to E$, tel que $\pi_u(P) = P(u) \cdot x$. On voit que $\pi_u^{-1}(F)$ est un idéal de $\mathbb{K}[X]$ qui contient l'idéal (μ_u), donc de la forme (D), avec D divise μ_u. Comme π_u est surjective, $F = \pi_u\big(\pi_u^{-1}(F)\big)$.

B.6. Exercice (Matrices avec un nombre fini de sous-espaces stables)
Soit u un endomorphisme d'un espace vectoriel E de dimension finie n sur un corps $\mathbb{K}$, supposé infini.

1. *Montrer que les conditions suivantes sont équivalentes :*
   (i) l'endomorphisme u a un nombre fini de sous espaces stables ;
   (ii) le polynôme caractéristique de u est égal à son polynôme minimal ;
   (iii) il existe x dans E tel que $\big(x, u(x), \dots, u^{n-1}(x)\big)$ soit une base de l'espace E.

   On pourra utiliser la décomposition de Frobenius. D'une part, pour montrer par la contraposée que (i) implique (ii), qui utilise $\mathbb{K}$ infini, d'autre part pour montrer (ii) implique (iii). Pour montrer que (iii) implique (i), on pourra utiliser l'exercice B.5.
2. *Montrer que si le corps est $\mathbb{C}$, alors cette condition définit un ouvert de l'espace des endomorphismes.*
   La condition *(iii)* est la plus maniable. Pour tout x de E, l'ensemble des u tels que $\det\big(x, u(x), \dots, u^{n-1}(x)\big) \neq 0$ est un ouvert. La réunion pour $x \in E$ de ces ouverts est encore un ouvert.

B.7. Exercice (Sous-espaces stables pour un endomorphisme cyclique)

Soit E un $\mathbb{K}$-espace et soit u un endomorphisme cyclique de $E = \mathbb{K}[u] \cdot x$ pour un x de E. On veut montrer qu'il existe une bijection entre l'ensemble $\mathscr{S}_u$ des sous-espaces stables par u et l'ensemble $\mathscr{D}_u$ des diviseurs unitaires du polynôme minimal μ_u de u. En particulier, on aura le résultat classique que l'ensemble des sous-espaces stables est fini pour les endomorphismes cycliques.

1. *Soit $F \in \mathscr{S}_u$ et soit $\pi : E \to E/F$ la surjection canonique.*
   (a) *Montrer que*
   $$\pi \circ u : E \to E/F$$
   passe au quotient en un endomorphisme u^F de E/F.
   (b) *Montrer que le polynôme minimal $D_F = \mu_{u^F}$ de u^F est dans $\mathscr{D}_u$.*
   (c) *Soit y dans E, et soit P_y un polynôme tel que $y = P_y(u)(x)$. Montrer que si $y \in F$, alors D_F divise P_y.*
   Projeter y dans le quotient par F et conclure.
   (d) *En déduire que l'on a : $F = \mathbb{K}[X]D_F(u)(x)$.*
2. *Réciproquement, soit D un diviseur unitaire de μ_u et soit F_D le sous-espace $\mathbb{K}[u]D(u)(x)$.*
   (a) *Montrer que D_{F_D} divise D.*
   (b) *Montrer que si $P(u)$ envoie x sur F_D, alors, en notant Q un polynôme tel que $P(u)(x) = Q(u)D(u)(x)$, le polynôme μ_u divise $P - QD$.*
   (c) *En déduire l'égalité $D_{F_D} = D$.*
   Poser $P = D_{F_D}$ pour obtenir que (D divise) μ divise $D_{F_D} - QD$.
3. *Conclure : les applications $F \mapsto D_F$ et $D \mapsto F_D$ sont des bijections réciproques entre $\mathscr{S}_u$ et $\mathscr{D}_u$.*

B.8. Exercice (Matrices nilpotentes avec un nombre fini de sous-espaces stables)

1. *Quels sont les sous-espaces stables d'une matrice nilpotente cyclique ?*
   C'est dans l'exercice B.6.
2. *Montrer que sur un corps infini, une matrice nilpotente possède un nombre fini de sous-espaces stables si et seulement si elle est cyclique.*
   Pour le « seulement si », on peut remarquer qu'une matrice nilpotente non cyclique possède un noyau de dimension > 1.

B.9. Exercice. *Soit E un espace vectoriel sur un corps $\mathbb{K}$ et soit u un endomorphisme de E. Soient F et F' deux sous-espaces de E stables par u.*

1. *Soit v un morphisme de E dans F' qui commute avec u. Montrer que v s'étend en un endomorphisme de E qui commute avec u.*
2. *On suppose u semi-simple. Soit v un morphisme de F dans E qui commute avec u, au sens où : $u \circ v = v \circ u_F$. Montrer que v se prolonge en un endomorphisme de E qui commute avec u.*
3. *On suppose encore u semi-simple. Montrer que tout isomorphisme v de F vers F' qui commute avec u se prolonge en un automorphisme de E qui commute avec u.*
   On pourra faire une décomposition de Frobenius de F pour u à laquelle on appliquera l'isomorphisme v. On complétera ensuite la décomposition de F en une décomposition de E.

B.10. Exercice (Classification des sous-espaces stables)

Si u est un endomorphisme de E dont les facteurs invariants sont donnés par les polynômes $(F_1, \dots, F_s)$ de $\mathbb{K}[X]$. On adopte les notations du corollaire A.13 de sorte que l'on a la suite exacte de $\mathbb{K}[X]$-modules :

$$0 \longrightarrow \mathbb{K}[X]^s \xrightarrow{\psi_M} \mathbb{K}[X]^s \xrightarrow{\phi_M} M \longrightarrow 0.$$

Soit F un sous-espace u-stable de E. On note M (resp. N) le $\mathbb{K}[X]$-module associé à E (resp. F). Soient $(G_1, \dots, G_{s'})$ les facteurs invariants de u_F.

1. *On pose $r = \max\{s, s'\}$. On a le diagramme commutatif de $\mathbb{K}[X]$-modules suivant :*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{K}[X]^r & \xrightarrow{\psi_M} & \mathbb{K}[X]^r & \xrightarrow{\phi_M} & M & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{Id}_{\mathbb{K}[X]^r}}\downarrow\!\downarrow & & {\scriptstyle \alpha_N}\uparrow & & {\scriptstyle \iota_N}\uparrow & & \\ 0 & \longrightarrow & \mathbb{K}[X]^r & \xrightarrow{\psi_N} & \mathbb{K}[X]^r & \xrightarrow{\phi_N} & N & \longrightarrow & 0, \end{array}$$

   où ι_N désigne l'injection naturelle et, pour $(P_1, \dots, P_r) \in \mathbb{K}[X]^r$,

$$\phi_M(P_1, \dots, P_r) = \sum_{i=1}^{s} P_i \cdot x_i,$$
$$\psi(P_1, \dots, P_r) = (F_1 P_1, \dots, F_s P_s, P_{s+1}, \dots, P_r),$$

   et avec les formules analogues pour N. Montrer que les suites du haut et du bas restent exactes après prolongement, et que l'on peut construire le morphisme α_N qui fasse commuter le diagramme.
   L'existence de α_N provient du fait que $\mathbb{K}[X]^r$ est libre, donc projectif, voir exercice III-E.3.
2. *En déduire que pour tout i, G_i divise F_i, en particulier, que $s' \leqslant s$.*
   Les morphismes entre les modules libres $\mathbb{K}[X]^r$ peuvent s'écrire matriciellement dans la base canonique. En notant A_N la matrice de α_N,

la commutation du diagramme donne $A_N \begin{pmatrix} G_1 & & \\ & \ddots & \\ & & \end{pmatrix} = \begin{pmatrix} F_1 & & \\ & \ddots & \\ & & \end{pmatrix}$ et donc A_N est diagonale et les G_i divisent les F_i.

3. *Réciproquement, on fixe $(G_1, \dots, G_{s'})$, $s' \leqslant s$, tel que G_i divise F_i et G_i divise G_{i-1} pour tout i. Montrer qu'il existe un sous-espace u-stable F de E tel que les facteurs invariants de u_F soient donnés par les G_i.*
Soit R_i tel que $R_i G_i = F_i$; alors, le sous-espace u-stable engendré par les $R_i \cdot x_i$ satisfait aux hypothèses.

B.11. Exercice (Orbites des u-stables pour l'action du commutant)

On reprend les hypothèses et les notations de l'exercice B.10. Soit GL_u le commutant de u dans $\mathrm{GL}(E)$. On fixe une famille de polynômes $\mathrm{G} = (G_1, \dots, G_{s'})$, $s' \leqslant s$, telle que G_i divise F_i et G_i divise G_{i-1} pour tout i. On note $\mathrm{Gr}_{u,\mathrm{G}}$ l'ensemble des sous-espaces u-stables F de E tels que les facteurs invariants de u_F soient donnés par la famille G.

1. *Montrer que GL_u agit naturellement sur $\mathrm{Gr}_{u,\mathrm{G}}$, par $g \cdot F = g(F)$.*
Comme g, inversible, commute avec u, il établit un isomorphisme de $\mathbb{K}[X]$-modules entre F et $g \cdot F$. On peut aussi le voir de façon plus pragmatique en disant que g envoie une décomposition de Frobenius de F en une décomposition de Frobenius de $g \cdot F$.

2. *Soit $E = \mathbb{K}^3$ et soit u de matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ dans une base (e_1, e_2, e_3). Montrer que les facteurs invariants de u sont $\big((X-1)^2, (X-1)\big)$, puis prouver que l'action de GL_u sur $\mathrm{Gr}_{u,(X-1)}$ n'est pas transitive.*
On obtient après calculs (ou pas !) qu'il y a deux orbites : la droite $\mathbb{K}e_1$ et l'ensemble des droites $\mathbb{K}(e_3 + ke_1)$ $(k \in \mathbb{K})$.

Petit débriefing. La non transitivité vient d'un non-théorème de la base incomplète[14]. Contrairement à ce qui se passait dans le cadre de l'exercice B.9, il n'y a pas semi-simplicité et donc un $\mathbb{K}[X]$-morphisme entre F et $g \cdot F$ ne se relève pas en un $\mathbb{K}[X]$-endomorphisme de E. Toutes ces choses se dissipent (avec lente alchimie) lors de l'apprentissage de la cohomologie des $\mathbb{K}[X]$-modules.

Analogue discret du bicommutant

On donne une version pour les groupes abéliens de la proposition 2.4 et du théorème 2.12.

B.12. Exercice. *Soient a et b des entiers. On note $H(a,b)$ le groupe des morphismes de groupes de $\mathbb{Z}/a\mathbb{Z}$ vers $\mathbb{Z}/b\mathbb{Z}$. Montrer que l'on a : $H(a,b) \simeq \mathbb{Z}/d\mathbb{Z}$, où d est le pgcd de a et b.*

[14] Un peu comme le non-anniversaire de Lewis Caroll.

B.13. Exercice. *Soit $(d_1, \dots, d_r)$ une suite finie d'entiers avec $d_i \mid d_{i+1}$ pour tout i entre 1 et $r-1$. On note M le groupe abélien $\bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$. On note $\mathrm{End}_{\mathbb{Z}}(M)$ le groupe des morphismes de groupe de M dans M et $\mathscr{C}^2$ le centre de $\mathrm{End}_{\mathbb{Z}}(M)$ — c'est le bicommutant de $\mathbb{Z}$ dans M. Montrer que $\mathscr{C}^2 = \mathbb{Z}\,\mathrm{Id}$.*

On choisit un générateur e_i de $\mathbb{Z}/d_i\mathbb{Z}$ pour tout i. Montrer que pour i compris entre 2 et r, il existe un unique élément $\varphi_i \in \mathrm{End}_{\mathbb{Z}}(M)$ tel que $\varphi_i(e_i) = e_{i-1}$ et $\varphi_i(e_j) = 0$ si $j \neq i$. On fixe $\theta \in \mathscr{C}^2$ et l'on note k l'entier tel que la r-ième composante de $\theta(e_r)$ vaut ke_r. Montrer que θ est parfaitement déterminé par la donnée de k.

Cône nilpotent

B.14. Exercice (Engendrement du cône nilpotent)

1. *Montrer que tout matrice carrée de trace nulle, sur un corps $\mathbb{K}$ de caractéristique nulle, est semblable à une matrice à diagonale nulle.*

   Par hypothèse sur le corps, la matrice, disons A, si elle est non nulle, n'est pas une homothétie. Donc, il existe un vecteur v de l'espace tel que (v, Av) est libre, voir [H2G2, proposition II-4.3.6]. En prenant un base qui prolonge cette famille libre, on voit que A est semblable à une matrice $\left(\begin{smallmatrix} 0 & * \\ * & N \end{smallmatrix}\right)$, avec N de trace nulle. On fait donc une récurrence, qui roule tranquille.

2. *En déduire que le cône nilpotent $\mathscr{N}$ engendre le sous-espace des matrices de trace nulle. En particulier, sur $\mathbb{R}$ et $\mathbb{C}$, il est d'intérieur vide.*

   Une inclusion est triviale. Pour l'autre, on se ramène, donc, par conjugaison à montrer qu'une matrice à diagonale nulle est engendrée par le cône nilpotent. Cela est clair, puisqu'elle est engendrée par les matrices élémentaires $E_{i,j}$ $(i \neq j)$ bien « cônues » pour être dans $\mathscr{N}$.

Réduction sur $\mathbb{Z}$

B.15. Exercice (Matrices entières d'ordre fini (approche))

1. *Montrer que si A est une matrice de $\mathscr{M}_n(\mathbb{Z})$ telle que $A^n = \mathrm{I}_n$, alors le polynôme caractéristique de A est un produit de polynômes cyclotomiques Φ_k avec k divisant n.*

   Toute racine du polynôme caractéristique est une racine n-ième de 1 et donc, dont le polynôme minimal sur $\mathbb{Z}$ est un polynôme cyclotomique.

2. *Montrer à l'aide des propriétés élémentaires de l'indicatrice d'Euler, que si le degré de Φ_n est égal à 1 ou 2, alors $n \in \{1, 2, 3, 4, 6\}$.*

3. *Déduire des questions qui précèdent qu'une matrice de $\mathscr{M}_2(\mathbb{Z})$ d'ordre fini est d'ordre 1, 2, 3, 4 ou 6.*

4. Décrire toutes les matrices de $\mathscr{M}_2(\mathbb{Z})$ d'ordre fini.
On cherchera leurs invariants de similitude, qui s'écrivent avec des polynômes cyclotomiques.

B.16. Exercice (Matrices de $\mathscr{M}_2(\mathbb{Z})$ de polynôme caractéristique fixé)

Soient a et b des entiers. On note $\mathscr{M}(a,b)$ l'ensemble des matrices A de $\mathscr{M}_2(\mathbb{Z})$ dont le polynôme caractéristique est : $\chi_A = (X-a)(X-b)$.

1. On suppose $a < b$. Montrer que $\mathscr{M}(a,b)$ possède exactement $b-a$ orbites pour l'action par conjugaison de $\mathrm{GL}_2(\mathbb{Z})$, un représentant pour chaque orbite étant donné par

$$\begin{pmatrix} a & i \\ 0 & b \end{pmatrix},\ 0 \leqslant i < b-a.$$

En travaillant d'abord sur $\mathbb{Q}$, montrer que si $\chi_A = (X-a)(X-b)$, alors il existe un vecteur propre $v_a = (x,y)$, avec x, y deux entiers premiers entre eux, pour la valeur propre a. Puis, utiliser la relation de Bézout pour trouver une matrice de passage P dans $\mathrm{GL}_n(\mathbb{Z})$ telle que

$$P^{-1}AP = \begin{pmatrix} a & z \\ 0 & b \end{pmatrix}.$$

2. Montrer que $\mathscr{M}(a,a)$ possède une infinité d'orbites pour l'action par conjugaison de $\mathrm{GL}_2(\mathbb{Z})$, un représentant pour chaque orbite étant

$$\begin{pmatrix} a & i \\ 0 & a \end{pmatrix} \quad (i \leqslant 0).$$

B.17. Exercice (Classes de similitude entières)

En utilisant l'exercice B.16, montrer que si $\mathscr{O}$ est une $\mathrm{GL}_n(\mathbb{Q})$-classe de similitude de $\mathscr{M}_n(\mathbb{Q})$, alors $\mathscr{O} \cap \mathscr{M}_n(\mathbb{Z})$ n'est pas toujours une $\mathrm{GL}_n(\mathbb{Z})$-classe de similitude.

B.18. Exercice (Classes de similitude de matrices entières nilpotentes)

En utilisant l'exercice B.16, montrer que pour $n \geqslant 2$, $\mathscr{M}_n(\mathbb{Z})$ possède une infinité d'orbites nilpotentes pour l'action par conjugaison de $\mathrm{GL}_n(\mathbb{Z})$.

B.19. Exercice. *Pour tout polynôme unitaire χ de degré n, soit $\mathrm{SS}_n(\chi,\mathbb{Z})$ l'ensemble des matrices de $\mathscr{M}_n(\mathbb{Z})$ qui sont semi-simples,* i.e. *dont l'endomorphisme associé est semi-simple, et dont le polynôme caractéristique est χ. Le but de cet exercice est de montrer qu'il n'y a qu'un nombre fini d'orbites dans $\mathrm{SS}_n(\chi,\mathbb{Z})$ pour l'action par conjugaison de $\mathrm{GL}_n(\mathbb{Z})$.*

1. *Montrer que si V est un sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{Q}^n$, alors $V \cap \mathbb{Z}^n$ est facteur direct dans le groupe abélien $\mathbb{Z}^n$.*
   On introduira une base adaptée pour $V \cap \mathbb{Z}^n$ et on étudiera ses facteurs invariants.
2. *Soit φ une application $\mathbb{Q}$-linéaire de $\mathbb{Q}^n$ vers $\mathbb{Q}^m$. Montrer que $\varphi(\mathbb{Z}^n)$ est un sous-groupe d'indice fini dans $\operatorname{im}\varphi \cap \mathbb{Z}^m$.*
   On montrera que pour tout x de $\operatorname{im}\varphi \cap \mathbb{Z}^m$, il existe un entier a tel que $ax \in \varphi(\mathbb{Z}^n)$, et l'on utilisera alors le théorème de la base adaptée.
3. *Montrer que si une matrice N de $\mathscr{M}_r(\mathbb{Z})$ est simple de polynôme caractéristique χ_N (donc irréductible sur $\mathbb{Q}$), alors N est $\mathrm{GL}_n(\mathbb{Z})$-semblable à la matrice compagnon C_{χ_N}. Montrer qu'il n'y a qu'une seule orbite dans le cas où χ est irréductible.*
4. *On suppose maintenant que χ n'est pas irréductible et que Q est un diviseur irréductible de χ de degré r. En utilisant la question 1, montrer qu'une matrice N de $\mathscr{M}_n(\mathbb{Z})$ telle que $\chi_N = \chi$ est $\mathrm{GL}_n(\mathbb{Z})$-semblable à M de la forme $\left(\begin{smallmatrix} A & Z \\ 0 & A' \end{smallmatrix}\right)$, où $A \in \mathscr{M}_r(\mathbb{Z})$ est une matrice simple telle que $\chi_A = Q$.*
5. *Soient $A \in \mathscr{M}_r(\mathbb{Z})$ et $A' \in \mathscr{M}_{r'}(\mathbb{Z})$. On considère le $\mathbb{Q}$-endomorphisme $\varphi : \mathscr{M}_{r,r'}(\mathbb{Q}) \to \mathscr{M}_{r,r'}(\mathbb{Q})$ tel que $\varphi(X) = XA' - AX$. Soient $M = \left(\begin{smallmatrix} A & Z \\ 0 & A' \end{smallmatrix}\right)$ et $M' = \left(\begin{smallmatrix} A & Z' \\ 0 & A' \end{smallmatrix}\right)$ les matrices de $\mathscr{M}_n(\mathbb{Z})$ avec $n = r+r'$. Montrer que si $Z' - Z \in \varphi\big(\mathscr{M}_{r,r'}(\mathbb{Q})\big)$, alors M et M' sont $\mathrm{GL}_n(\mathbb{Z})$-semblables.*
   On pourra utiliser une matrice de passage de la forme $\left(\begin{smallmatrix} \mathrm{I}_r & X \\ 0 & \mathrm{I}_{r'} \end{smallmatrix}\right)$.
6. *On suppose maintenant la matrice M semi-simple. On veut montrer que l'on a : $Z \in \operatorname{im}\varphi \cap \mathscr{M}_{r,r'}(\mathbb{Z})$.*
   (a) *Montrer que A et A' sont également semi-simples et que M est $\mathrm{GL}_n(\mathbb{Q})$-semblable à $S = \left(\begin{smallmatrix} A & 0 \\ 0 & A' \end{smallmatrix}\right)$.*
   (b) *Montrer que si une matrice de passage $P = \left(\begin{smallmatrix} Q & R \\ 0 & Q' \end{smallmatrix}\right)$ de $\mathrm{GL}_n(\mathbb{Q})$ vérifie $PMP^{-1} = S$, alors $Z \in \operatorname{im}\varphi \cap \mathscr{M}_{r,r'}(\mathbb{Z})$.*
   (c) *Conclure en utilisant l'exercice B.9.*
7. *En utilisant la question 2, montrer par récurrence sur le nombre de simples de la décomposition que $\mathrm{SS}_n(\chi, \mathbb{Z})$ est réunion finie d'orbites.*

B.20. Exercice. *On veut étudier la finitude du nombre d'orbites de l'action de $\mathrm{GL}_n(\mathbb{Z})$ par conjugaison sur l'ensemble $\mathscr{M}_n(\chi, \mathbb{Z})$ des matrices $n \times n$ à coefficients entiers de polynôme caractéristique χ unitaire de degré n dans $\mathbb{Z}[X]$.*

1. *Dans cette question la décomposition de χ en irréductibles de $\mathbb{Z}[X]$ n'a pas de multiplicité. Montrer en utilisant le résultat de l'exercice précédent que le nombre d'orbites est fini.*

2. *On suppose ici que $\chi = Q^2$ avec Q irréductible sur $\mathbb{Z}$ de degré r. Pour tout $k \in \mathbb{Z}$, on pose*

$$M_k = \begin{pmatrix} C_Q & k\mathrm{I}_r \\ 0 & C_Q \end{pmatrix},$$

où C_Q est la matrice compagnon du polynôme Q.

   (a) *Montrer qu'il existe deux polynômes U et V de $\mathbb{Z}[X]$ et d dans $\mathbb{K}[X]$ tels que $UQ + VQ' = d$.*

   (b) *On choisit k premier avec d. Montrer que si p premier divise k, alors la réduction $\overline{M}_k$ de M_k modulo p est semi-simple.*

   (c) *Réciproquement, montrer que si $\overline{M}_{k'}$ est semi-simple modulo p, alors $\overline{C}_Q\overline{X} - \overline{X}\overline{C}_Q = \overline{k}\overline{\mathrm{I}}_r$ et ainsi p divise $k'r$.*

   On s'inspirera du 6) de l'exercice précédent. Pour la dernière question, prendre la trace.

   (d) *En déduire qu'il existe une infinité d'orbites dans $\mathscr{M}_n(\chi, \mathbb{Z})$.*

   On choisit k premier avec r et k' premier avec k et r. Alors, p ne divise pas $k'r$. Donc, $\overline{M}_{k'}$ n'est pas semblable à $\overline{M}_k$ et ainsi $M_{k'}$ n'est pas $\mathrm{GL}_n(\mathbb{Z})$-semblable à M_k.

3. *Montrer alors le cas général : si χ a une multiplicité, alors $\mathscr{M}_n(\chi, \mathbb{Z})$ possède une infinité d'orbites.*

   On pourra chercher des représentants de la forme $\left(\begin{smallmatrix} M_k & 0 \\ 0 & B \end{smallmatrix}\right)$ et quotienter, en s'assurant que B reste aussi semi-simple que possible modulo p.

That many dreams within dreams is too unstable!
Christopher Nolan, *Inception*, 2010.

Chapitre III

Problèmes d'algèbre linéaire

What's next? On pourrait imaginer qu'à ce stade, les objets fondamentaux de l'algèbre linéaire sont bel et bien rangés, classifiés, mesurés et répertoriés[1]. En effet, nous avons classifié les espaces par la dimension, les applications linéaires par le rang, les endomorphismes par les valeurs propres et les tableaux de Young, les invariants de similitude... On peut également classer des familles de droites du plan à l'aide du birapport, des paires de drapeaux par le groupe symétrique.

Nous allons voir que tous ces problèmes se fondent en un seul, bien plus vaste et ambitieux. On pourrait même dire qu'il s'agit là de la généralisation *ad libitum* de la théorie de la réduction des endomorphismes, voire *du* problème universel de l'algèbre linéaire, mais l'abus d'une boisson énergisante à une heure tardive est peut-être à l'origine de cette révélation. Quoiqu'il en soit, l'expression faussement naïve « problèmes d'algèbre linéaire » pour désigner cet ensemble de problèmes a été popularisée par Peter Gabriel.

Commençons, comme première étape vers la généralisation, par deux problèmes classiques : le problème de classification des configurations et le théorème de Jordan-Kronecker.

La classification des configurations. Nous avons vu dans [H2G2, proposition X-1.2.7], que trois droites deux à deux distinctes du plan (vectoriel), sur un corps $\mathbb{K}$, peuvent s'écrire $\mathbb{K}e_1$, $\mathbb{K}e_2$, $\mathbb{K}(e_1+e_2)$, où (e_1,e_2) est une base du plan, unique à homothétie près. Autrement dit, l'action de $\mathrm{GL}_2(\mathbb{K})$ sur $\mathbb{P}^1(\mathbb{K})$ est trois fois transitive, ce qui signifie aussi que les orbites pour l'action naturelle de $\mathrm{GL}_2(\mathbb{K})$ sur $\mathbb{P}^1(\mathbb{K})^3$ sont au nombre de cinq, selon les égalités des droites du triplet entre elles (par exemple, on a une orbite

[1] Par « linéaire », on sous-entend que l'on reste en degré 1, bien entendu. La classification des formes quadratiques sur un corps quelconque garde tout son mystère.

constituée des triplets (D, D', D) avec $D \neq D'$). Qu'en est-il d'un quadruplet de droites ? On se rend compte que le groupe $\mathrm{GL}_2(\mathbb{K})$ a atteint ses limites puisque le quotient $\mathbb{P}^1(\mathbb{K})^4/\mathrm{GL}_2(\mathbb{K})$ est maintenant infini (si le corps est infini) et, de plus, un invariant pour quatre droites a été dégagé dans le tome premier : un élément de $\mathbb{P}^1(\mathbb{K})$ nommé le birapport. Cet invariant est suffisamment fécond pour que l'on tente de généraliser la démarche : on veut donc classer les *configurations* de l'espace, c'est-à-dire la donnée de k sous-espaces $(F_1, \ldots, F_k)$ d'un espace vectoriel E, modulo $\mathrm{GL}(E)$. Les cas $k = 1$ et $k = 2$ sont simples à comprendre ; ils n'utilisent qu'une formulation attendue du théorème de la base incomplète. Mais pour $k = 3$, le problème est plus ardu ; toutefois, tant que E reste fixé, le classifiant reste fini. En revanche, comme on peut s'y attendre pour le cas des droites dans le plan, le cas $k = 4$, donne un classifiant infini, mais peut toutefois être « domestiqué ».

Le théorème de Jordan-Kronecker. De même, le problème suivant généralise de façon naturelle le problème de classification des applications linéaires. On fixe deux espaces E et F, un entier positif m, et l'on se propose de classer $\mathscr{L}(E, F)^m$ modulo changement de base de E et F, c'est-à-dire modulo l'action naturelle de $\mathrm{GL}(E) \times \mathrm{GL}(F)$. Ce problème se résout à l'aide du rang dans le cas $m = 1$, mais pour le cas $m = 2$, il se révèle beaucoup plus ardu. Dans ce cas, le théorème de Jordan-Kronecker donne quand même une classification dont la combinatoire reste assez simple. On y rencontre les célèbres blocs de Jordan dont l'origine remonte à cette étude. La preuve proposée de ce résultat est certes imposante, mais elle reste élémentaire.

Généralisation. Tous ces problèmes évoqués trouvent une généralisation élégante[2] dans la notion de représentation de carquois, introduite par Peter Gabriel. En bref, un carquois est un graphe orienté, c'est-à-dire un objet constitué de sommets et de flèches (d'où son nom) orientées, une chose somme toute assez rudimentaire. Une représentation d'un carquois Q est la donnée d'un espace E_i attaché à chaque sommet i et d'applications linéaires f_{ij} de E_i à E_j pour chaque flèche de i à j. Le « problème » est de classer les représentations de Q modulo l'action naturelle du groupe $\prod_i \mathrm{GL}(E_i)$. On pourra effectivement voir sur des exemples et en exercices que la classification des représentations de carquois permet de retrouver, à la fois, les théorèmes sur les applications linéaires, des configurations, des endomorphismes, et des n-uplets de drapeaux. Mais comme on peut s'y attendre, l'entreprise est audacieuse et les preuves sont loin d'être élémentaires[3]. Mais comme dit Goethe, « l'audace a du génie, du pouvoir,

[2] On finit par s'en convaincre.

[3] Pour en apprendre plus sur le sujet, le livre [72], qui vient de sortir, est très recommandable. Outre le contenu de ce chapitre, on y trouve un nombre considérable d'exemples et la théorie d'Auslander-Reiten qui, malgré son abstraction apparente, per-

de la magie ». Ainsi, nous avons dû invoquer quelques esprits non élémentaires : on trouvera en annexe, quelques rations de A-modules, un soupçon d'extension et d'algèbre homologique (limitée au degré 1), quelques gouttes de géométrie différentielle dans le contexte des groupes de Lie, et enfin, une dose homéopathique mais puissante de géométrie algébrique. On en aura parcouru du chemin depuis le pivot de Gauss, non ?

1. Problèmes des N sous-espaces

Pour fixer les idées, on travaillera ici sur $\mathbb{C}$, mais tout autre corps ferait l'affaire dans cette partie.

Soit N un entier naturel. On appelle *configuration de N sous-espaces* la donnée d'un espace vectoriel E et de N sous-espaces $F_1, \dots, F_N$. Un *morphisme de configurations* (resp. un isomorphisme de configurations) de $(E; F_1, \dots, F_N)$ vers $(E'; F'_1, \dots, F'_N)$ est une application linéaire (resp. une application linéaire bijective) $\varphi : E \to E'$ telle que $\varphi(F_i) \subset F'_i$ (resp. $\varphi(F_i) = F'_i$) pour tout i. Une sous-configuration de $(E; F_1, \dots, F_N)$ est une configuration $(E'; F'_1, \dots, F'_N)$ où E' est un sous-espace de E et $F'_i = E' \cap F_i$ pour tout i. La somme directe de deux configurations $(E; F_1, \dots, F_N)$ et $(E'; F'_1, \dots, F'_N)$ est $(E \oplus E'; F_1 \oplus F'_1, \dots, F_N \oplus F'_N)$. Une configuration est dite *indécomposable* si elle n'est pas isomorphe à la somme de deux sous-configurations non triviales.

Résoudre le problème des N sous-espaces, c'est trouver une classification des configurations à isomorphisme près, ce qui revient à classer les indécomposables. Avec l'approche des A-modules et le théorème de Krull-Schmidt A.14, on verra en effet pourquoi une décomposition est unique à isomorphisme et à l'ordre des facteurs directs près.

1.1. Exemple. Si $n = 0$, la classification des espaces vectoriels à isomorphisme près est donnée par la dimension ; la seule configuration indécomposable est $\mathbb{C}$, *l'*espace de dimension 1.

1.2. Exemple (Trois droites en dimension 2). Soit $E = \mathbb{C}^2$ muni de sa base canonique (e_1, e_2), soient α et β deux scalaires, et soient F_1, F_2, F_3 les droites engendrées respectivement par e_1, e_2 et $\alpha e_1 + \beta e_2$. On veut décomposer les configurations $(\mathbb{C}^2; F_1, F_2, F_3)$.

Si $(\alpha, \beta) = (0, 0)$, on a : $(\mathbb{C}^2; F_1, F_2, F_3) \simeq (\mathbb{C}; \mathbb{C}, 0, 0) \oplus (\mathbb{C}; 0, \mathbb{C}, 0)$.

Si $(\alpha, \beta) \in \{0\} \times \mathbb{C}^*$, on a : $(\mathbb{C}^2; F_1, F_2, F_3) \simeq (\mathbb{C}; \mathbb{C}, 0, 0) \oplus (\mathbb{C}; 0, \mathbb{C}, \mathbb{C})$.

---

met de mettre de l'ordre dans les représentations indécomposables et fournit des algorithmes puissants pour les calculer — le diagramme (AR) du §1.5 (p. 119) relève de cette théorie.

Si $(\alpha, \beta) \in \mathbb{C}^* \times \mathbb{C}^*$, alors $(\mathbb{C}^2 ; F_1, F_2, F_3)$ est indécomposable. Sinon, pour des raisons de dimension, il se décomposerait en $(\mathbb{C} ; \mathbb{C}, 0, 0) \oplus (\mathbb{C} ; 0, \mathbb{C}, \mathbb{C})$ ou en $(\mathbb{C} ; 0, 0, 0) \oplus (\mathbb{C} ; \mathbb{C}, \mathbb{C}, \mathbb{C})$, quitte à échanger le rôle de F_1 et F_2. Le premier est impossible car cela signifierait que $F_3 = F_2$, le second encore plus puisqu'il entraîne $F_1 = F_2 = F_3$.

En revanche, vérifions que tous les couples (α, β) de $\mathbb{C}^* \times \mathbb{C}^*$, les configurations correspondantes sont isomorphes. En effet, soit F la droite engendrée par $e_1 + e_2$, alors l'isomorphisme $\mathbb{C}^2 \to \mathbb{C}^2$ qui envoie e_1 sur αe_1 et e_2 sur βe_2 envoie $(\mathbb{C}^2 ; F_1, F_2, F)$ sur $(\mathbb{C}^2 ; F_1, F_2, F_3)$. On retrouvera cette classe d'isomorphisme de configuration indécomposable dans la suite ; elle sera notée conventionnellement $(\mathbb{C}^2 ; \mathbb{C}, \mathbb{C}, \mathbb{C})$.

1.3. Cas d'un sous-espace

Le problème se représente ainsi :

$$F_1 \hookrightarrow E.$$

Le cas d'un seul sous-espace est aussi très facile et, à vrai dire, a déjà été traité, mais dans d'autres termes... On doit classer les drapeaux $(E ; F_1)$ formés d'un espace et un sous-espace. Partant d'une base $(e_1, \ldots, e_m)$ de F_1, on la complète en une base $(e_1, \ldots, e_n)$ de E. Il est immédiat que $(E ; F_1)$ est la somme directe des configurations $(\mathbb{C}e_i ; \mathbb{C}e_i)$ $(1 \leqslant i \leqslant m)$ et $(\mathbb{C}e_j ; 0)$ $(m + 1 \leqslant j \leqslant n)$. De plus, le couple (m, n) ne dépend que du drapeau et pas du choix de la base.

Ainsi, le couple

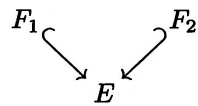
$$(\dim F_1, \dim E) \in \{(m, n) \in \mathbb{N} \times \mathbb{N},\ m \leqslant n\}$$

est un invariant (il est préservé par isomorphisme) et même un invariant complet, c'est-à-dire que deux couples sont isomorphes si et seulement s'ils sont associés aux mêmes dimensions. De plus, les configurations indécomposables sont $(\mathbb{C} ; 0)$ et $(\mathbb{C} ; \mathbb{C})$.

Si l'on veut procéder matriciellement, il faut fixer la dimension n de l'espace ambiant E et la dimension m du sous-espace F. Choisissons aussi une base $\mathbf{e} = (e_1, \ldots, e_n)$ de E et une base de F dont on écrit les colonnes de coordonnées dans la base $\mathbf{e}$. Les opérations élémentaires sur les rangées de la matrice $n \times m$ obtenue s'interprètent en termes de changement de base dans E (manipulations sur les lignes) ou dans F (manipulations sur les colonnes), donc elles ne changent pas la classe d'isomorphisme du couple (F, E). Grâce à l'algorithme du pivot de Gauss, on transforme la matrice en la matrice $\mathrm{I}_{m,n,m}$ du premier chapitre (rappelons que son rang est m). Autrement dit, le couple (F, E) est dans la classe d'isomorphisme du sous-espace engendré par les m premiers vecteurs de la base canonique de $\mathbb{C}^n$.

1.4. Cas de deux sous-espaces

Le problème se représente ainsi :



Prenons ici deux sous-espaces F_1 et F_2. Assurément, les dimensions de E, F_1, F_2, $F_1 \cap F_2$ et $F_1 + F_2$ sont invariantes par isomorphisme. La formule dite de Grassmann établit une relation entre ces données :

$$\dim(F_1 + F_2) = \dim F_1 + \dim F_2 - \dim(F_1 \cap F_2),$$

si bien que trois des quatre entiers permettent de retrouver le quatrième.

Proposition (Problème des deux sous-espaces). *Les triplets* $(E\,; F_1, F_2)$ *formés d'un espace et de deux sous-espaces sont classés, à isomorphisme près, par le quadruplet*

$$\big(\dim E, \dim F_1, \dim F_2, \dim(F_1 \cap F_2)\big),$$

qui peut prendre n'importe quelle valeur dans

$$\big\{(n, d_1, d_2, d_{12}) \in \mathbb{N}^4,\ d_{12} \leqslant \min(d_1, d_2) \text{ et } \max(d_1, d_2) \leqslant n\big\}.$$

Démonstration. Première méthode. On a déjà remarqué que les dimensions étaient invariantes par isomorphisme. Il reste alors à vérifier que deux triplets $(E\,; F_1, F_2)$ et $(E'\,; F_1, F_2)$ ayant les mêmes dimensions (n, d_1, d_2, d_{12}) sont isomorphes.

Soit $\mathbf{u}$ une base de $F_1 \cap F_2$. On la complète en une base[4] $\mathbf{u} \cup \mathbf{v}_1$ de F_1 et en une base $\mathbf{u} \cup \mathbf{v}_2$ de F_2. Comme dans la preuve de la formule de Grassmann, on vérifie que $\mathbf{u} \cup \mathbf{v}_1 \cup \mathbf{v}_2$ est une base de $F_1 + F_2$. On la complète en une base $\mathbf{u} \cup \mathbf{v}_1 \cup \mathbf{v}_2 \cup \mathbf{w}$ de E. On construit de même une base $\mathbf{u}' \cup \mathbf{v}_1' \cup \mathbf{v}_2' \cup \mathbf{w}'$ de E'. L'application linéaire qui envoie une base sur l'autre est un isomorphisme de $(E\,; F_1, F_2)$ sur $(E'\,; F_1', F_2')$.

Deuxième méthode. On fixe les dimensions n, p et q de E, F_1 et F_2. On choisit une base $(u_1, \ldots, u_n)$ de E et des familles génératrices des sous-espaces, $(v_1, \ldots, v_p)$ et $(w_1, \ldots, w_q)$. Puis, on écrit les colonnes de coordonnées des familles génératrices de F_1 et F_2 dans la base de E. On obtient une matrice

[4] Il y a un abus de notation à employer une réunion pour des bases, qui sont des familles ordonnées et non pas des ensembles. *Be it!*

rectangulaire $n \times (p+q)$ coupée en deux blocs de tailles $n \times p$ et $n \times q$:

$$A = (B|C) = \left(\begin{array}{ccc|cc} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \end{array}\right).$$

Un changement de la base de E se traduit par des manipulations sur les lignes de la matrice. Un changement de base dans F_1 ou F_2 se traduit par des opérations sur les colonnes de la matrice qui ne font intervenir que les p premières ou les q dernières colonnes — on ne peut pas mélanger les vecteurs de F_1 et de F_2. Ces opérations ne changent pas la classe d'isomorphisme du triplet $(E; F_1, F_2)$. Autrement dit, on est en train de considérer l'action du groupe $\mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_p(\mathbb{C}) \times \mathrm{GL}_q(\mathbb{C})$ sur $\mathscr{M}_{n,p+q}(\mathbb{C})$ définie, avec des notations naturelles, par :

$$(g, g_1, g_2) \cdot (B|C) = (gBg_1^{-1}|gCg_2^{-1}).$$

Trouvons une forme normale pour la matrice $A = (B|C)$ pour cette action. D'abord, par des opérations sur les lignes et sans se préoccuper pour l'instant de la séparation entre les blocs, on transforme A en une matrice échelonnée (en lignes) :

$$\left(\begin{array}{cccc|cccc} 0 & 1 & 0 & * & 0 & * & 0 & * \\ 0 & 0 & 1 & * & 0 & * & 0 & * \\ 0 & 0 & 0 & 0 & 1 & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Par des opérations sur les colonnes, on peut annuler les coefficients situés à droite d'un pivot et dans le même bloc : on se ramène à la forme suivante :

$$\left(\begin{array}{cccc|cccc} 0 & 1 & 0 & 0 & 0 & * & 0 & * \\ 0 & 0 & 1 & 0 & 0 & * & 0 & * \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Les coefficients qui restent indéterminés sont les coefficients situés dans le bloc de droite, sur la ligne d'un pivot du bloc de gauche mais pas situés au-dessus d'un pivot du bloc de droite. Sur une ligne où apparaît un coefficient de ce type, on appelle pivot secondaire le coefficient non nul situé le plus à gauche (il est cependant dans le bloc de droite).

Considérons le pivot secondaire le plus haut. Quitte à diviser la colonne dans laquelle il se trouve par ce qu'il faut, on peut supposer qu'il vaut 1.

Par des combinaisons linéaires portant sur les colonnes du bloc de droite, on annule tous les coefficients qui se situent sur la même ligne, à droite de ce pivot secondaire :

$$\left(\begin{array}{cccc|cccc} 0&1&0&0&0&1&0&0\\ 0&0&1&0&0&*&0&*\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0 \end{array}\right).$$

En faisant une combinaison linéaire des *lignes*, on annule tous les coefficients situés sous le pivot secondaire : cela fait en général apparaître des coefficients non nuls dans le bloc de gauche :

$$\left(\begin{array}{cccc|cccc} 0&1&0&0&0&1&0&0\\ 0&*&1&0&0&0&0&*\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0 \end{array}\right).$$

Par des combinaisons linéaires portant sur les colonnes du bloc de gauche, on annule les coefficients que l'on vient de créer :

$$\left(\begin{array}{cccc|cccc} 0&1&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&*\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0 \end{array}\right).$$

Le nombre de coefficients indéterminés a ainsi strictement diminué. On continue de la sorte jusqu'à ce que chaque ligne contienne soit un 1 et les autres coefficients nuls, soit un 1 dans chaque bloc et les autres coefficients nuls, avec la contrainte qu'il y a au plus un 1 dans chaque colonne. En réordonnant lignes et colonnes, on obtient la matrice par blocs :

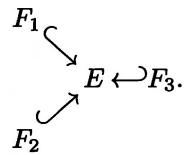
$$\left(\begin{array}{cccc|cccc} \mathrm{I}_{d_{12}}&&&&\mathrm{I}_{d_{12}}&&&\\ &\mathrm{I}_{d_1-d_{12}}&&&&0&&\\ &&0&&&&\mathrm{I}_{d_2-d_{12}}&\\ &&&0&&&&0 \end{array}\right).$$

Sur une telle forme, on voit que les d_{12} premiers vecteurs de la base de E forment une base de $F_1 \cap F_2$, les d_1 premiers vecteurs une base de F_1, les vecteurs d'indice $1 \leqslant i \leqslant d_{12}$ et $d_1 + 1 \leqslant i \leqslant d_1 + d_2 - d_{12}$ une base de F_2. La fin de la preuve est laissée aux bons soins du lecteur patient. □

Corollaire. *Les indécomposables dans le problème des deux sous-espaces sont :* $(\mathbb{C};\mathbb{C},\mathbb{C})$, $(\mathbb{C};\mathbb{C},0)$, $(\mathbb{C};0,\mathbb{C})$, $(\mathbb{C};0,0)$.

1.5. Cas de trois sous-espaces

On peut représenter le problème ainsi :



Les configurations indécomposables de trois sous-espaces sont plus compliquées mais restent, on va le voir, en nombre fini. Soit $(E\,;F_1,F_2,F_3)$ une configuration. Commençons par étudier les cas de petite dimension, lorsque l'on a : $\dim E \leqslant 2$.

Lorsque E est une droite, la situation est simple. Chaque sous-espace F_i est $\{0\}$ ou E, ce qui donne huit configurations :

$$(\mathbb{C}\,;\mathbb{C},\mathbb{C},\mathbb{C}),\quad (\mathbb{C}\,;\mathbb{C},\mathbb{C},0),\quad (\mathbb{C}\,;\mathbb{C},0,\mathbb{C}),\quad (\mathbb{C}\,;0,\mathbb{C},\mathbb{C}),$$
$$(\mathbb{C}\,;\mathbb{C},0,0),\quad (\mathbb{C}\,;0,\mathbb{C},0),\quad (\mathbb{C}\,;0,0,\mathbb{C}),\quad (\mathbb{C}\,;0,0,0)\,.$$

On peut noter que chacune est caractérisée par la dimension des sous-espaces.

Lorsque E est un plan, plusieurs configurations dégénèrent en configurations de deux sous-espaces. En effet, si l'un des sous-espaces, disons F_3, est réduit à $\{0\}$, à E ou à un autre des sous-espaces F_j $(1 \leqslant j \leqslant 2)$, on étudie la configuration $(E\,;F_1,F_2)$, ce que l'on sait faire, puis l'on ajoute benoîtement le sous-espace $\{0\}$, E ou F_j. Une telle configuration est nécessairement somme directe de deux indécomposables, chacune de l'un des types précédents. Rien de bien nouveau à attendre de la sorte.

Toujours lorsque E est un plan, on suppose donc désormais que les trois sous-espaces sont des droites distinctes. On fixe une base e_1 de F_1, une base e_2 de F_2. Alors, (e_1,e_2) est une base de E et F_3 est engendré par une combinaison linéaire $\alpha e_1+\beta e_2$ avec $\alpha\beta\neq 0$. Quitte à remplacer e_1 par αe_1 et e_2 par βe_2, on peut supposer que $\alpha=1=\beta$. On voit que la configuration est isomorphe à :

$$\big(\mathbb{C}e_1\oplus\mathbb{C}e_2\,;\mathbb{C}e_1,\mathbb{C}e_2,\mathbb{C}(e_1+e_2)\big).$$

On notera $(\mathbb{C}^2\,;\mathbb{C},\mathbb{C},\mathbb{C})$ cette configuration. Elle est indécomposable : si l'on écrit E comme somme directe de deux sous-espaces $E'\oplus E''$, au moins l'une des droites F_i aura une intersection triviale avec E' et E'', si bien que la configuration ne sera pas la somme des sous-configurations.

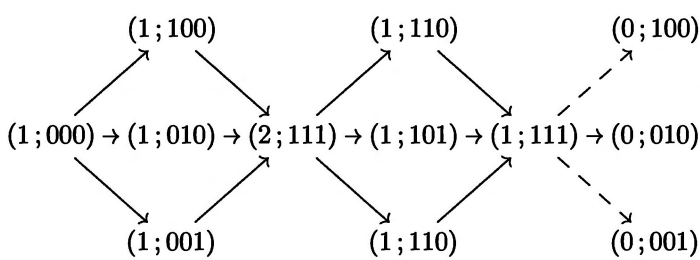
Voici un exemple où toutes les configurations mises en évidence ci-dessus apparaissent une fois dans la somme directe en indécomposables :

- E est l'espace engendré par dix vecteurs $e_1, \ldots, e_{10}$;
- $F_1 = \mathrm{Vect}(e_2, e_5, e_8, e_9, e_{10})$;
- $F_2 = \mathrm{Vect}(e_3, e_6, e_7, e_9, e_{10})$;
- $F_3 = \mathrm{Vect}(e_4, e_5 + e_6, e_7, e_8, e_{10})$;

La donnée d'une famille de vecteurs engendre un sous-espace vectoriel E', ce qui détermine une sous-configuration $(E' ; E' \cap F_1, E' \cap F_2, E' \cap F_3)$. Ici, on vérifie sans peine que :

- le vecteur e_1 détermine une configuration de type $(\mathbb{C} ; 0, 0, 0)$;
- le vecteur e_2 détermine une configuration de type $(\mathbb{C} ; \mathbb{C}, 0, 0)$;
- le vecteur e_3 détermine une configuration de type $(\mathbb{C} ; 0, \mathbb{C}, 0)$;
- le vecteur e_4 détermine une configuration de type $(\mathbb{C} ; 0, 0, \mathbb{C})$;
- les vecteurs e_5 et e_6 déterminent une configuration de type $(\mathbb{C}^2 ; \mathbb{C}, \mathbb{C}, \mathbb{C})$;
- le vecteur e_7 détermine une configuration de type $(\mathbb{C} ; 0, \mathbb{C}, \mathbb{C})$;
- le vecteur e_8 détermine une configuration de type $(\mathbb{C} ; \mathbb{C}, 0, \mathbb{C})$;
- le vecteur e_9 détermine une configuration de type $(\mathbb{C} ; \mathbb{C}, \mathbb{C}, 0)$;
- le vecteur e_{10} détermine une configuration de type $(\mathbb{C} ; \mathbb{C}, \mathbb{C}, \mathbb{C})$.

Notons $(d ; a, b, c)$ ou même $(d ; abc)$ une configuration $(\mathbb{C}^d ; \mathbb{C}^a, \mathbb{C}^b, \mathbb{C}^c)$ qui apparaît ci-dessus. On peut écrire certains morphismes de configurations dans un diagramme :



(AR)

En fait, le diagramme ci-dessus contient beaucoup d'informations. Par exemple, tout morphisme de configurations est somme de composées des morphismes dans le diagramme mais il y a beaucoup d'autres choses cachées dans ce que l'on appelle un carquois d'Auslander-Reiten, voir [6, Chapter 4].

Nous allons montrer que nous connaissons déjà toutes les configurations indécomposables. Pour cela, nous allons en quelque sorte éplucher une configuration quelconque en faisant apparaître les indécomposables en procédant de la droite vers la gauche dans le diagramme ci-dessus.

1.6. Proposition. *Toute configuration de trois sous-espaces est somme directe des configurations indécomposables suivantes :*

$$(\mathbb{C}^2;\mathbb{C},\mathbb{C},\mathbb{C}),\quad (\mathbb{C};\mathbb{C},\mathbb{C},\mathbb{C}),\quad (\mathbb{C};\mathbb{C},\mathbb{C},0),\quad (\mathbb{C};\mathbb{C},0,\mathbb{C}),\quad (\mathbb{C};0,\mathbb{C},\mathbb{C}),$$
$$(\mathbb{C};\mathbb{C},0,0),\quad (\mathbb{C};0,\mathbb{C},0),\quad (\mathbb{C};0,0,\mathbb{C}),\quad (\mathbb{C};0,0,0).$$

(Dans la première configuration, les trois droites sont distinctes.)

Démonstration. Soit $(E;F_1,F_2,F_3)$ une configuration. On pose :

$$\begin{aligned} F &= F_1+F_2+F_3,\\ G &= F_1\cap(F_2+F_3)+F_2\cap(F_1+F_3)+F_3\cap(F_1+F_2),\\ H &= F_2\cap F_3+F_1\cap F_3+F_1\cap F_2,\\ K &= F_1\cap F_2\cap F_3. \end{aligned}$$

On a : $K\subset H\subset G\subset F$. Remarquons d'ores et déjà que $(E;F_1,F_2,F_3)$ admet $\dim(K)$ sous-configurations isomorphes à $(\mathbb{C};\mathbb{C},\mathbb{C},\mathbb{C})$.

Soit H_1' un supplémentaire de K dans $F_2\cap F_3$. On définit de même H_2' et H_3'. On a : $F_1\cap F_2=K+H_3'$, d'où la relation : $H=K+H_1'+H_2'+H_3'$. En fait, la somme est directe : si l'on a une relation $w+v_1+v_2+v_3=0$ avec $w\in K$ et $v_i\in H_i'$, alors il vient : $v_1=-w-v_2-v_3\in F_1$, d'où $v_1\in K$ et donc $v_1=0$. De même, v_2 et v_3 sont nuls, d'où enfin : $w=0$. Ainsi :

$$H=K\oplus H_1'\oplus H_2'\oplus H_3'.$$

Notons

$$G_1=F_1\cap(F_2+F_3),\quad G_2=F_2\cap(F_1+F_3),\quad G_3=F_3\cap(F_1+F_2).$$

1.7. Lemme. *Avec les notations ci-dessus, on a :*

(i) $G_3\subset G_1+G_2$, *c'est-à-dire que* $G=G_1+G_2$;

(ii) $G_1\cap G_2=F_1\cap F_2$;

(iii) $H\cap G_1=F_1\cap F_2+F_1\cap F_3$, $H\cap G_2=F_2\cap F_1+F_2\cap F_3$,

(iv) $H=H\cap G_1+H\cap G_2$.

Démonstration (du lemme). (i) Soit $w\in G_3$, on écrit $w=u+v$ avec $u\in F_1$ et $v\in F_2$. Alors, on a : $u=-v+w\in F_2+F_3$, d'où on tire que $u\in G_1$. De même, on montre que $v\in G_2$, d'où : $w\in G_1+G_2$.

(ii) L'assertion est immédiate.

(iii) Soit $v\in H\cap G_1$, on écrit : $v=v_{12}+v_{13}+v_{23}$ où $v_{ij}\in F_i\cap F_j$. On a : $v_{23}=v-v_{12}-v_{13}\in F_1$ donc $v_{23}\in F_1\cap F_2\cap F_3\subset F_1\cap F_2$. On en déduit : $v\in F_1\cap F_2+F_1\cap F_3$. L'inclusion réciproque est évidente et l'on procède de même avec $H\cap G_2$.

(iv) L'assertion est évidente. □

Revenons à la proposition. Pour $i \in \{1,2,3\}$, on choisit un supplémentaire G'_i de $H \cap G_i$ dans G_i. On définit $f : G_3 \to G'_1$ et $g : G_3 \to G'_2$ de la façon suivante. Pour $w \in G_3$, on écrit, par le lemme, $w = u+v$ avec $u \in G_1$ et $v \in G_2$. Si $w = u' + v'$ est une autre décomposition de cette forme, on a : $u' - u = v - v' \in G_1 \cap G_2 \subset H$. Par suite, la projection de u sur G'_1 (resp. de v sur G'_2) parallèlement à H ne dépend que de w : on la note $f(w)$ $\big($resp. $g(w)\big)$.

Montrons que f et g se restreignent en des injections notées encore f : $G'_3 \to G'_1$ et $g : G'_3 \to G'_2$. Soit w un vecteur de G'_3 qui annule f. Avec les notations précédentes, $u \in H \cap G_1 = F_1 \cap F_2 + F_1 \cap F_3$. On écrit $u = u_{12}+u_{13}$, avec $u_{1j} \in F_1 \cap F_j \subset G_j$. On a : $w - u_{13} = u_{12} + v \in G_3 \cap G_2 \subset H$. Mais comme $u_{13} \in H$, il vient : $w \in H$, si bien que $w = 0$. On procède de même pour g.

On vient de prouver l'inégalité $\dim G'_3 \leqslant \dim G'_1$. Par symétrie, les dimensions de G'_1, G'_2 et G'_3 sont égales. De plus, le lemme 1.7 implique l'égalité

$$G = H \oplus G'_1 \oplus G'_2.$$

En effet, d'une part, on a :

$$\begin{aligned} H + G'_1 + G'_2 &= H + H + G'_1 + G'_2 = (H + G'_1) + (H + G'_2) \\ &= H + G_1 + G_2 = H + G = G. \end{aligned}$$

D'autre part, supposons avoir $h \in H$, $g'_1 \in G'_1$ et $g'_2 \in G'_2$ tels que $h + g'_1 + g'_2 = 0$. Alors, $g'_2 = -h - g'_1 \in (H + G'_1) \cap G_2 = G_1 \cap G_2 \subset H$. Par suite, $g'_2 = 0$ et, de même, $g'_1 = 0$, et enfin : $h = 0$. La somme est donc directe.

Montrons que $G'_1 \oplus G'_2$ est isomorphe à la somme directe de $\dim(G'_3)$ copies de $(\mathbb{C}^2\,;\mathbb{C},\mathbb{C},\mathbb{C})$ (et, en particulier, que la dimension de G/H est paire, chose que l'on peut vérifier par un calcul vaguement pénible mais qui ne saute pas aux yeux *a priori*.)

Pour cela, fixons une base (w_k) de G'_3. On pose $u_k = f(w_k)$ et $v_k = g(w_k)$ pour tout k. Alors, (u_k) est une base de G'_1 et (v_k) est une base de G'_2. Pour k entre 1 et $\dim G'_3$, le sous-espace C_k engendré par u_k, v_k est de dimension 2 et contient $w_k = u_k + v_k$. C'est donc une configuration isomorphe à $(\mathbb{C}^2\,;\mathbb{C},\mathbb{C},\mathbb{C})$. Comme (u_k) est une base de G'_1, que (v_k) est une base de G'_2 et que G'_1 et G'_2 sont en somme directe, l'espace $G'_1 \oplus G'_2$ est bien la somme directe des sous-espaces C_k $(1 \leqslant k \leqslant \dim G'_3)$.

Ensuite, on choisit un supplémentaire F'_i de $F_i \cap G$ dans F_i. On a :

$$F = F_1 + F_2 + F_3 = G \oplus F'_1 \oplus F'_2 \oplus F'_3.$$

Vérifions-le. D'une part, on a :

$$G + F'_1 + F'_2 + F'_3 = (G + F'_1) + (G + F'_2) + (G + F'_3) = F_1 + F_2 + F_3 = F.$$

D'autre part, soient $g \in G$ et $f'_i \in F'_i$ $(1 \leqslant i \leqslant 3)$ tels que $g + f'_1 + f'_2 + f'_3 = 0$.

Alors, $g + f_1' \in F_1$ et donc : $f_3' = -(g + f_1') - f_2' \in F_1 \cap F_2$. Avec $f_3' \in F_3$, cela entraîne que $f_3' \in G$, si bien que $f_3' = 0$. De même, $f_1' = f_2' = 0$. La somme est donc directe.

Enfin, on choisit un supplémentaire E' de $F_1 + F_2 + F_3$ dans E. Au bilan :

$$E = E' \oplus F_1' \oplus F_2' \oplus F_3' \oplus (G_1' \oplus G_2') \oplus H_1' \oplus H_2' \oplus H_3' \oplus K.$$

On reconnaît, dans l'ordre, des sous-configurations isomorphes à $(\mathbb{C}\,;0,0,0)$, $(\mathbb{C}\,;\mathbb{C},0,0)$, $(\mathbb{C}\,;0,\mathbb{C},0)$, $(\mathbb{C}\,;0,0,\mathbb{C})$, $(\mathbb{C}^2\,;\mathbb{C},\mathbb{C},\mathbb{C})$, $(\mathbb{C}\,;0,\mathbb{C},\mathbb{C})$, $(\mathbb{C}\,;\mathbb{C},0,\mathbb{C})$, $(\mathbb{C}\,;\mathbb{C},\mathbb{C},0)$, $(\mathbb{C}\,;\mathbb{C},\mathbb{C},\mathbb{C})$.

1.8. Remarque. L'idée pour les cas de zéro, un, ou deux sous-espaces (on parlera bientôt des types A_1, A_2, A_3) a été de ramener ces problèmes de configurations de sous-espaces à des problèmes de configurations ensemblistes grâce à des adaptations du théorème de la base incomplète.

Pour le cas de trois sous-espaces (on dira plus tard D_4), cela est impossible : on se rend compte que les équivalents ensemblistes des sous-espaces notés F et G sont identiques alors que ce sont des espaces en général différents. Pour être plus précis, prenons $E = \mathbb{C}^2$ et fixons trois droites F_1, F_2, F_3 deux à deux distinctes de E ; on a :

$$G = F_1 \cap (F_2 + F_3) + F_2 \cap (F_1 + F_3) + F_3 \cap (F_1 + F_2) = E,$$
$$H = F_2 \cap F_3 + F_1 \cap F_3 + F_1 \cap F_2 = \{0\}.$$

Dans ce cas, on a d'une part :

$$\dim(F_1 + F_2 + F_3) = 2,$$

et, en revanche :

$$\dim F_1 + \dim F_2 + \dim F_3 - \dim(F_1 \cap F_2) - \dim(F_1 \cap F_3) - \dim(F_2 \cap F_3) + \dim(F_1 \cap F_2 \cap F_3) = 3.$$

Force est de constater que l'analogie entre sous-espaces et sous-ensembles que nous laissait espérer la formule de Grassmann n'est qu'une fallacieuse promesse : on ne peut plus, à partir de trois sous-espaces, raisonner avec des patates ! Toute la complexité de ce dernier résultat (et la catastrophe annoncée au §3) réside peut-être dans cette remarque.

1.9. Cas de quatre sous-espaces et plus

Une surprise apparaît : dès que l'espace ambiant est de dimension supérieure ou égale à 2, il y a, une infinité de configurations indécomposables, même à isomorphisme près.

Illustrons cela en dimension 2 lorsque les quatre sous-espaces sont des droites. Si au moins deux d'entre elles coïncident, on a affaire à un problème déjà traité. Supposons donc qu'elles soient distinctes : classer quatre droites

dans $\mathbb{C}^2$ à isomorphisme près, c'est exactement classer quatre points dans $\mathbb{P}^1$ à homographie près. Or on sait, par [H2G2, proposition X-1.2.16], que les orbites de quatre points de $\mathbb{P}^1$ sous l'action de $\mathrm{PSL}_2(\mathbb{C})$ sont classées par le birapport, qui peut prendre n'importe quelle valeur dans $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

La solution générale du problème des quatre sous-espaces est due à Gel'fand et Ponomarev [35]. On se contente de dire que, comme en dimension 2, on a pour toute dimension un nombre fini de configurations indécomposables dépendant d'un paramètre.

Il y a pire : dès que l'on essaie de classer les situations indécomposables pour cinq sous-espaces ou plus, on s'aperçoit que le problème est *de type sauvage*. On précisera ce que cela veut dire au paragraphe 3.

1.10. Remarque (Treillis modulaires)

Étant donnés des sous-espaces $F_1, \ldots, F_r$ d'un espace E, combien peut-on définir de sous-espaces avec les opérations $+$ et $\cap$? Outre[5] E et $\{0\}$, on peut former :

- si $r = 1$: le seul sous-espace F_1 ;
- si $r = 2$: les quatre sous-espaces $F_1 \cap F_2$, F_1, F_2, $F_1 + F_2$;
- si $r = 3$: vingt-six sous-espaces en général (et donc vingt-huit en tout), comme l'a montré Richard Dedekind dès l'année 1900 dans [20] ;
- si $r = 4$: une infinité d'espaces *a priori*, a prouvé George Birkhoff dans [7] (mais bien sûr, un nombre fini dans chaque espace de dimension finie).

Le bon cadre pour poser ces questions est celui des *treillis*. Un treillis (*lattice* en anglais) est un ensemble partiellement ordonné où toute paire d'éléments possède une borne supérieure et une borne inférieure. Par exemple, les parties d'un ensemble forment un treillis pour l'inclusion : la borne supérieure est la réunion, la borne inférieure l'intersection ; il est de plus distributif, au sens où l'intersection et la réunion sont distributives l'une sur l'autre.

Les sous-espaces d'un espace vectoriel forment aussi un treillis : la borne supérieure est la somme, la borne inférieure l'intersection. Mais il n'est pas distributif : en général, il est faux de dire que $X+(Y\cap Z) = (X+Y)\cap Z$. En revanche, cette égalité est satisfaite si l'on suppose que $X \subset Z$: elle définit alors la notion de *treillis modulaire*. Le treillis modulaire libre $\mathrm{FM}(r)$ sur r générateurs « est » l'ensemble des expressions que l'on peut former à partir de r sous-espaces avec les opérations $+$ et $\cap$. Le résultat de Dedekind (resp. de Birkhoff) exprime que $\mathrm{FM}(3)$ admet vingt-huit éléments (resp. $\mathrm{FM}(4)$ est infini). Il y a pire. D'après Ralph Freese [28], le problème du mot n'est pas résoluble dans $\mathrm{FM}(5)$: il s'agit d'un résultat d'indécidabilité semblable à celui que l'on va rencontrer dans le paragraphe 3, p. 133.

[5] De même qu'il faut poser $\sum_{i\in\emptyset} a_i = 0$ pour avoir $\sum_{i\in I\cup J} a_i = \sum_{i\in I} a_i + \sum_{i\in J} a_i$ pour tout couple de parties disjointes (I, J) et toute famille $(a_i)_{i\in I\cup J}$, il est naturel de poser : $E = \bigcap_{i\in\emptyset} F_i$ et $\{0\} = \sum_{i\in\emptyset} F_i$.

2. Le théorème de Jordan-Kronecker

« Der Tee ist gut aber meine Tasse ist zu klein » :
« L'amitié franco-allemande est le plus sûr garant de la paix en Europe »,
écrivait Schopenhauer.

Pierre Desproges, *Le tribunal des flagrants délires*, 1980.

Mettant un terme aux désaccords franco-allemands nés de la guerre de 1870 puis de la controverse de 1874 qui opposa Camille Jordan et Leopold Kronecker — dûment détaillée dans [13] — la communauté mathématique contribua enfin à restaurer la paix dans le monde lorsqu'elle eut l'idée lumineuse d'unir les sus-nommés dans un théorème unique.

Après avoir trouvé les invariants pour les endomorphismes à conjugaison près, il peut paraître dans la logique des choses de chercher à comprendre des invariants pour les couples d'endomorphismes à conjugaison près, c'est-à-dire pour l'action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathscr{M}_n(\mathbb{K})\times\mathscr{M}_n(\mathbb{K})$ donnée par $P\cdot(A,B)=(PAP^{-1},PBP^{-1})$. Un petit résultat bien connu est la codiagonalisation de deux matrices diagonalisables (ou plus) qui commutent deux à deux.

2.1. Proposition. *Soient A et B deux matrices diagonalisables sur un corps $\mathbb{K}$. Alors, A et B commutent si et seulement si elles sont diagonalisables dans une base commune.*

Démonstration. Deux matrices diagonales commutent. Inversement, supposons que A et B commutent. Comme A est diagonalisable, l'espace est la somme directe des sous-espaces propres K_λ pour A et comme A et B commutent, chaque K_λ est stable par B (si vous n'avez pas encore démontré ce grand classique, c'est le moment ou jamais). La restriction de (l'endomorphisme de multiplication par) A à K_λ est une homothétie donc toute base est propre. Il suffit donc de trouver une base de K_λ propre pour B. La restriction B_{K_λ} de B à K_λ est un endomorphisme et son polynôme minimal divise celui de B. Ce dernier étant scindé simple puisque B est diagonalisable, le polynôme minimal de B_{K_λ} est aussi scindé simple et donc B_{K_λ} est diagonalisable. □

2.2. Remarque. On laisse le soin au lecteur de généraliser cette preuve par récurrence — sur la dimension — pour une famille quelconque de matrices diagonalisables qui commutent.

Malheureusement, une classification des orbites sans l'hypothèse de diagonalisabilité semble impossible, voir le paragraphe 3.

En revanche, le théorème du rang exprime que pour classer les applications linéaires à changement de base au départ et à l'arrivée près, le rang est un

invariant total, si bien qu'il n'y a qu'un nombre fini d'orbites. La simplicité de ce résultat nous encourage vivement à autoriser des changements de base différents au départ et à l'arrivée.

Autrement dit, on veut étudier les orbites de l'action de $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$ sur $\mathscr{M}_{n,m}(\mathbb{K}) \times \mathscr{M}_{n,m}(\mathbb{K})$ donnée par $(P,Q)\cdot(A,B) = (PAQ^{-1}, PBQ^{-1})$. Le théorème de Jordan-Kronecker donne une réponse complète à ce problème.

On notera dans la suite $(A,B) \sim (A',B')$ lorsque les deux couples sont dans la même orbite. Afin de simplifier l'énoncé du théorème de Jordan-Kronecker, tel que l'on pourrait le trouver dans [6], nous allons déjà le transposer naturellement en une action du produit $\mathrm{GL}(E) \times \mathrm{GL}(F)$ sur l'espace des couples d'applications linéaires $\mathscr{L}(E,F) \times \mathscr{L}(E,F)$, où E et F sont des espaces de dimensions respectives m et n. Cela permet d'introduire la notion de couple indécomposable $(\alpha,\beta) \in \mathscr{L}(E,F) \times \mathscr{L}(E,F)$ pour l'action.

2.3. Définition. Un couple (α,β) de $\mathscr{L}(E,F) \times \mathscr{L}(E,F)$ est dit *décomposable* s'il existe une décomposition $E = E_1 \oplus E_2$, $F = F_1 \oplus F_2$, non triviale pour au moins l'un des deux espaces telle que $\alpha(E_i) \subset F_i$ et $\beta(E_i) \subset F_i$ pour $i = 1,2$. Dans ce cas, on dit que $(E_1,F_1) \oplus (E_2,F_2)$ est une décomposition pour (A,B). On étend la notion à un nombre quelconque de couples (E_i,F_i). Le couple est dit *indécomposable* s'il n'existe pas de telle décomposition.

On montre par récurrence sur la dimension que tout couple (α,β) d'applications linéaires admet une décomposition en indécomposables $(E_1,F_1) \oplus \cdots \oplus (E_t,F_t)$. Comme pour la factorisation des entiers, l'unicité d'une telle décomposition sera plus délicate à formuler et à prouver.

Par commodité, on pourra identifier (A,B) avec (α,β) si des bases de E et de F sont fixées. Matriciellement, décomposer le couple (A,B) revient à trouver P et Q telles que PAQ^{-1} et PBQ^{-1} soient diagonales par blocs, avec t blocs diagonaux de tailles $\dim(F_i) \times \dim(E_i)$ $(1 \leqslant i \leqslant t)$.

Par exemple, si l'on réduit la définition à une seule application linéaire[6], le théorème du rang dit que les seules orbites d'applications linéaires indécomposables sont les orbites de $\alpha_1 : 0 \to \mathbb{K}$, $\alpha_{12} : \mathbb{K} \to \mathbb{K}$, $1 \mapsto 1$, $\alpha_2 : \mathbb{K} \to 0$.

Bien entendu, par construction, si un couple est indécomposable, alors toute son orbite est constituée de couples d'indécomposables. On peut maintenant énoncer le *théorème de Jordan-Kronecker* en termes d'indécomposables.

[6]On peut par exemple oublier β, ou bien supposer que β est l'application nulle de sorte à faire disparaître toute contrainte.

2.4. Théorème (Jordan-Kronecker). *Soit* $\mathbb{K}$ *un corps algébriquement clos. Un ensemble non redondant de représentants des orbites de couples indécomposables* (A, B) *pour l'action du groupe produit* $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$ *sur* $\mathscr{M}_{n,m}(\mathbb{K}) \times \mathscr{M}_{n,m}(\mathbb{K})$ *est donné par les couples suivants :*

(i) $m = n+1$, $n \geqslant 0$,

$$A_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}, \qquad B_n = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix};$$

(ii) $n = m+1$, $m \geqslant 0$,

$${}^tA_n = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}, \qquad {}^tB_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \vdots & & \ddots & 1 \\ 0 & \cdots & \cdots & 0 \end{pmatrix};$$

(iii) $n = m$, $n \geqslant 1$,

$$A_n(\lambda) = \mathrm{I}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}, \qquad \begin{matrix} B_n(\lambda) = \\ \lambda \in \mathbb{K} \end{matrix} \begin{pmatrix} \lambda & 1 & & (0) \\ 0 & \ddots & \ddots & \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \lambda \end{pmatrix},$$

$$A_n(\infty) = \begin{pmatrix} 0 & 1 & & (0) \\ 0 & \ddots & \ddots & \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & 0 \end{pmatrix}, \qquad {}_n(\infty) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} = \mathrm{I}_n.$$

Démonstration. On laisse le soin au lecteur de montrer que les couples (A, B) sont bien indécomposables. Lançons le mouvement en montrant l'assertion pour le cas (i). On munit l'espace de départ E de la base (e_j), et l'espace d'arrivée F de la base (f_i), bases dans lesquelles les matrices A et B sont écrites. On suppose par l'absurde les décompositions $E = E' \oplus E''$, $F = F' \oplus F''$, avec A, B envoyant E' vers F' et E'' vers F'', avec (E', F'), (E'', F'') non triviaux. Comme $\mathrm{im}(A) + \mathrm{im}(B) = F$, il vient que si $E' = E$ alors $F' = F$, et ainsi (E'', F'') serait trivial. Donc, $E' \neq E$, et de même $E'' \neq E$, ce qui implique aussi que les espaces E' et E'' sont non nuls. On peut alors considérer un élément non nul v' (resp. v'') de E' (resp. de E''). Par une étude de cas (on en distingue trois : (a) $v' \in \mathbb{C}e_1$, (b) $v' \in \mathbb{C}e_{n+1}$, (c) $v' \notin \mathbb{C}e_1 \cup \mathbb{C}e_{n+1}$), on montre que soit il existe k tel que $A^k v' = f_1$, soit

il existe k tel que $B^k v' = f_1$. De même pour v''. Cela implique que f_1 est dans $F' \cap F''$: absurde. Les autres cas sont similaires.

On suppose que (A, B) est un couple indécomposable de matrices et l'on note (α, β) le couple de morphismes de E vers F correspondant pour une base de E et une base de F fixées.

Première étape : on suppose que $\dim E = \dim F = n$ et $\det A \neq 0$. Soit P une matrice de passage telle que $P(A^{-1}B)P^{-1}$ soit une réduite de Jordan J, ce qui existe puisque $\mathbb{K}$ est algébriquement clos ; la matrice J est alors unique. On a alors : $(PA^{-1}, P) \cdot (A, B) = (\mathrm{I}_n, J)$, d'où : $(\mathrm{I}_n, J) \sim (A, B)$. Comme (I_n, J) est indécomposable alors que I_n peut se décomposer dans toute partition d'une base, la matrice J est un bloc de Jordan indécomposable, que l'on peut choisir sous la forme $B_n(\lambda)$ de l'énoncé.

Deuxième étape : on suppose que $\dim E = \dim F$ et $\det(A + XB)$ est un polynôme non nul de $\mathbb{K}[X]$ (en fait, la suite montrera qu'il ne peut pas être nul). Comme $\mathbb{K}$ est algébriquement clos, il est infini et l'on peut trouver un scalaire $\mu \in \mathbb{K}$ tel que $\det(A + \mu B) \neq 0$. On peut supposer que A n'est pas inversible puisque si elle l'est, le problème est résolu par l'étape précédente ; il vient alors : $\mu \neq 0$.

Posons $A' = A + \mu B$ et $B' = A$. Alors, (A', B') est indécomposable car (A, B) l'est. D'après le cas précédent, on peut trouver (P, Q) dans $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$ et pour un λ de $\mathbb{K}$ tels que $(P, Q) \cdot (A', B') = \big(\mathrm{I}_n, B_n(\lambda)\big)$. Or, $B' = A$ n'est pas inversible, on a donc : $\lambda = 0$. Maintenant, par construction, on a : $B = \mu^{-1}(A' - B')$, d'où :

$$PBQ^{-1} = \mu^{-1}(PA'Q^{-1} - PB'Q^{-1}) = \mu^{-1}\big(\mathrm{I}_n - B_n(0)\big)\,.$$

Cette égalité implique que B est inversible. En intervertissant les rôles de A et B et en appliquant l'étape précédente, on obtient l'isomorphisme : $(A, B) \sim \big(A_n(\infty), B_n(\infty)\big)$.

Troisième étape : on suppose que $\dim E \neq \dim F$ ou que $\dim E = \dim F$ avec $\det(A + XB) = 0$. Dans cette situation, quitte à remplacer (A, B) par $({}^tA, {}^tB)$ lorsque $\dim E < \dim F$ (c'est encore un couple indécomposable (pourquoi ?)), on suppose que l'on a : $\dim(E) \geqslant \dim(F)$.

On identifie E à $\mathbb{K}^m$ et F à $\mathbb{K}^n$ via les bases dans lesquelles α et β ont pour matrices A et B. On introduit alors les espaces vectoriels $\mathbf{E} = \mathbb{K}(X)^m$ et $\mathbf{F} = \mathbb{K}(X)^n$ sur le corps des fractions rationnelles $\mathbb{K}(X)$. Ils héritent de bases provenant de celles de E et F.

On a supposé que la dimension de $\mathbf{E}$ est strictement supérieure à celle de $\mathbf{F}$ ou que le déterminant de $A + XB$ est nul : ainsi, $A + XB$ n'est pas injective, vue comme application $\mathbb{K}(X)$-linéaire de $\mathbf{E}$ vers $\mathbf{F}$.

Un vecteur v de $\mathbf{E} = \mathbb{K}(X)^n$ sera dit polynomial si ses coefficients dans la base distinguée ci-dessus sont des polynômes en X ; le degré de v est par définition le degré maximum de ses coefficients. Il existe un vecteur v non nul dans le noyau de $A+XB$, que l'on peut choisir polynomial en chassant les dénominateurs. On peut être plus précis grâce au lemme 2.5 énoncé ci-dessous.

Soit $d(A,B)$ le degré minimal d'un vecteur polynomial non nul du noyau de $A+XB$. On vient de voir que $d(A,B) \leqslant \mathrm{rg}(A+XB)$. Soit v un vecteur du noyau de degré $s = d(A,B)$; on l'écrit $v = v_0 - v_1X + v_2X^2 - \cdots + (-1)^s v_s X^s$, où $v_i \in E$ pour tout i. Quelques observations s'imposent :

1. par minimalité, v_0 et v_s ne sont pas nuls ;
2. le nombre $d(A,B)$ est invariant par l'action de $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$;
3. le nombre $d(A,B)$ a un sens sans hypothèses sur les dimensions de E et F si l'on convient que $d(A,B) = -\infty$ lorsque $A+XB$ est injective.

On rappelle que (A,B) est indécomposable. Nous allons montrer par récurrence sur $s = d(A,B)$ l'assertion

$$H_s \ : \quad (A,B) \sim (A_s, B_s).$$

Initialisation. Si $s = 0$ alors v_0 est un vecteur non nul de $\mathbb{K}^n$ et $(A+XB)v_0 = 0$, ce qui implique : $Av_0 = Bv_0 = 0$. Soit E' un hyperplan supplémentaire de $\mathbb{K}v_0$ dans E. Alors, $(\mathbb{K}v_0, \{0\}) \oplus (E', F)$ est une décomposition non triviale pour (A,B). Comme (A,B) est indécomposable, on obtient $E' = \{0\}$, $F = \{0\}$ et $(A,B) = (A_0, B_0)$ comme désiré.

Hérédité. On suppose que $d(A,B) = s$ et que H_i est vraie pour $i \leqslant s-1$. Commençons par construire deux nouvelles bases. L'égalité $(A+XB)v = 0$ implique la relation :

$$\begin{aligned} &Av_0 + X(Bv_0 - Av_1) + X^2(Bv_1 - Av_2) + \cdots \\ &\quad + (-1)^s X^s (Av_s - Bv_{s-1}) + (-1)^s X^{s+1} Bv_s = 0. \end{aligned}$$

Par identification, il vient : $Av_0 = 0$, $Av_1 = Bv_0, \ldots, Av_s = Bv_{s-1}, 0 = Bv_s$. Montrons que les vecteurs $Av_1, \ldots, Av_s$ sont libres sur $\mathbb{K}$. Soit $(x_1, \ldots, x_s)$ une s-liste de scalaires tels que $x_1Av_1 + \cdots + x_sAv_s = 0$. Posons alors

$$w_0 = x_s v_0, \ w_1 = x_{s-1}v_0 + x_s v_1, \ldots, \ w_{s-1} = x_1 v_0 + \cdots + x_s v_{s-1}.$$

Par élimination en cascade, on en tire :

$$(A+XB)\big(w_0 - w_1X + w_2X^2 + \cdots + (-1)^{s-1} w_{s-1} X^{s-1}\big) = 0,$$

ce qui donne un vecteur de degré strictement inférieur à s dans le noyau de $A+XB$: ce vecteur est nul, si bien que tous les w_i sont nuls. Comme v_0 n'est pas le vecteur nul, on voit de proche en proche que tous les scalaires x_i sont nuls.

On en déduit en particulier que $v_0, \dots, v_s$ sont linéairement indépendants. En effet, une relation $x_0v_0+\cdots+x_sv_s = 0$ implique $x_1Av_1+\cdots+x_sAv_s = 0$, et donc $x_1 = \cdots = x_s = 0$. Il reste : $x_0v_0 = 0$, d'où $x_0 = 0$ car v_0 n'est pas nul.

On construit donc deux bases, une base de E qui complète la partie libre $(v_0, \dots, v_s)$ et une de F qui complète $(Av_1, \dots, Av_s)$. Grâce à ces bases, on voit que la matrice $A + XB$ est $\mathbb{K}$-équivalente une matrice de la forme

$$\begin{pmatrix} A_s + XB_s & C + XD \\ 0 & A' + XB' \end{pmatrix},$$

avec $C, D \in \mathscr{M}_{s,\ell}(\mathbb{K})$, $A', B' \in \mathscr{M}_{m,\ell}(\mathbb{K})$, $m = \dim F - s$ et $\ell = \dim E - s - 1$. Montrons qu'il existe des matrices $R \in \mathscr{M}_{s,m}(\mathbb{K})$ et $S \in \mathscr{M}_{s+1,\ell}(\mathbb{K})$ telles que

$$\begin{pmatrix} \mathrm{I}_s & R \\ 0 & \mathrm{I}_m \end{pmatrix} \begin{pmatrix} A_s + XB_s & C + XD \\ 0 & A' + XB' \end{pmatrix} \begin{pmatrix} \mathrm{I}_{s+1} & S \\ 0 & \mathrm{I}_l \end{pmatrix} = \begin{pmatrix} A_s + XB_s & 0 \\ 0 & A' + XB' \end{pmatrix}.$$

Par identification et en utilisant le fait que (A, B) est un couple indécomposable, on obtiendra que $(A, B) \sim (A_s, B_s)$ comme désiré.

L'équation matricielle s'écrit $R(A' + XB') + (C + XD) + (A_s + XB_s)S = 0$. Après identification, on obtient une autre équation matricielle que l'on peut développer ligne par ligne en :

$$\begin{cases} R_iA' + C_i + S_{i+1} = 0 \\ R_iB' + D_i + S_i = 0, \end{cases}$$

où $1 \leqslant i \leqslant s$ et où l'on a noté M_i la i-ème ligne d'une matrice M. En éliminant les S_i $(2 \leqslant i \leqslant s)$, on obtient

$$\begin{cases} R_1B' + D_1 + S_1 = 0 \\ R_{i-1}A' + C_{i-1} - R_iB' - D_i = 0 \quad \text{pour } 2 \leqslant i \leqslant n \\ R_sA' + C_s + S_{s+1} = 0. \end{cases}$$

Soit T la matrice $sm \times (s-1)\ell$ donnée par

$$T = \begin{pmatrix} A' & & (0) \\ -B' & \ddots & \\ & \ddots & \ddots \\ & & \ddots \; A' \\ (0) & & -B' \end{pmatrix}.$$

Il suffit donc de trouver des solutions à l'équation en R_i de la forme

$$(R_1, R_2, \dots, R_s)T = M,$$

où M est une matrice dépendant des paramètres fixés (D_i, C_i...).

Il suffit de montrer que la matrice T est inversible à droite, c'est-à-dire que le noyau de ${}^tT$ est nul. Supposons au contraire qu'il existe un vecteur non nul $u = (u_{11}, \dots, u_{1m}, u_{21}, \dots, u_{sm})$ tel que ${}^tT\,{}^tu = 0$. Un calcul simple montre comme précédemment que le vecteur

$$w = \big(u_{11} - u_{21}X + \cdots + (-1)^{s-1}u_{s1}X^{s-1}, \dots \\ \dots, u_{1m} - u_{2m}X + \cdots + (-1)^{s-1}u_{sm}X^{s-1}\big)$$

satisfait à : $w(A' + XB') = 0$. Il vient ainsi : $({}^tA' + X\,{}^tB')\,{}^tw = 0$.

Notons que le degré de ${}^tw$ est au plus $s-1$, ce qui implique comme ci-dessus que $A' + XB'$ est $\mathbb{K}$-équivalente à

$$\begin{pmatrix} {}^tA_d + X\,{}^tB_d & 0 \\ C'' + XD'' & A'' + XB'' \end{pmatrix}, \quad \text{avec } 0 \leqslant d < s.$$

Ainsi, (A, B) est $\mathbb{K}$-équivalente à

$$\begin{pmatrix} A_s + XB_s & C^0 + XD^0 & C^1 + XD^1 \\ 0 & {}^tA_d + X\,{}^tB_d & 0 \\ 0 & C'' + XD'' & A'' + XB'' \end{pmatrix},$$

ce qui entraîne que $({}^tA, {}^tB)$ est $\mathbb{K}$-équivalente à

$$\begin{pmatrix} {}^tA_s + X\,{}^tB_s & 0 & 0 \\ {}^tC^0 + X\,{}^tD^0 & A_d + XB_d & {}^tC'' + X\,{}^tD'' \\ {}^tC^1 + X\,{}^tD^1 & 0 & {}^tA'' + X\,{}^tB'' \end{pmatrix}.$$

Or l'indécomposabilité de (A, B) implique celle de $({}^tA, {}^tB)$ et l'on a l'inégalité : $0 \leqslant d' = d({}^tA, {}^tB) \leqslant d < s$. Par hypothèse de récurrence, cela implique que $({}^tA, {}^tB) \sim (A_{d'}, B_{d'})$, ce qui est absurde à cause de la taille des matrices.

On a donc prouvé par l'absurde que le système possède des solutions en R et S : en d'autres termes, (A, B) est dans l'orbite de (A_s, B_s) et l'on a de plus : $n = s$.

Quatrième étape : conclusion (enfin !). Nous avons vu que si $\dim E = \dim F$, alors le polynôme $\det(A + XB)$ n'est pas nul, si bien que l'on se trouve dans le cas (iii). Si $\dim E < \dim F$, on reconnaît le cas (i) et par transposition, on montre que si $\dim E > \dim F$, on est dans le cas (ii) du théorème.

Par un argument de dimension, les cas (i), (ii) et (iii) s'excluent mutuellement. Enfin, on a vu que les couples $\big(A(\lambda), B(\lambda)\big)$ n'étaient pas dans la même orbite pour deux valeurs distinctes de $\lambda \in \mathbb{K} \cup \{\infty\}$. □

2.5. Lemme. *Soient A et B deux matrices de taille $n \times m$ sur $\mathbb{K}$. Si, comme application $\mathbb{K}(X)$-linéaire, $A+XB$ n'est pas injective et si son rang est r, alors le noyau de $A+XB$ contient un vecteur polynomial non nul de degré inférieur ou égal à r.*

Démonstration. On sait qu'il existe une sous-matrice carrée de $A+XB$ inversible de taille r. On peut supposer que cette sous-matrice correspond aux r premières rangées. On considère la matrice M correspondant aux $r+1$ premières lignes et $r+1$ premières colonnes. Elle est de rang r et sa comatrice est donc non nulle, et ses coefficients sont des polynômes de degré inférieur à r.

On a : $M\,{}^t\mathrm{com}(M) = 0$. Soit $u \in \mathscr{M}_{r+1,1}\big(\mathbb{K}(X)\big) = \mathbb{K}(X)^{r+1}$ une colonne non nulle de ${}^t\mathrm{com}(M)$. La colonne de même indice de $M\,{}^t\mathrm{com}(M)$ est : $Mu = 0$. Par définition de r, toutes les lignes de $A+XB$ sont combinaisons linéaires des r premières. Il suffit donc de prolonger u par des zéros pour obtenir un vecteur $v \in \mathbb{K}[X]^m$ non nul tel que $(A+XB)v = 0$; son degré est inférieur ou égal à r puisque ses coefficients non nuls sont des coefficients de $\mathrm{com}(M)$. □

On vient de montrer qu'à équivalence simultanée près, tout couple de matrices rectangulaires est une somme directe de certains des couples indécomposables de la liste du théorème 2.4. Dans ce genre de situation, on aime bien avoir unicité de la décomposition (penser au théorème de Jordan sans Kronecker). Pour cela, un peu d'abstraction ne nuit pas : en interprétant le problème en termes des représentations du carquois $\bullet \rightrightarrows \bullet$ comme dans l'exemple 4.11, on peut appliquer le corollaire A.16. Voici ce que l'on obtient.

2.6. Théorème. *Soit (A,B) un couple de matrices rectangulaires. Alors (A,B) se décompose comme une somme directe de couples indécomposables $(A_i,B_i)_{1\leqslant i\leqslant s}$. Cette décomposition est unique au sens suivant : si $(A'_i,B'_i)_{1\leqslant i\leqslant s'}$ est une autre décomposition, alors $s=s'$ et il existe une permutation $\sigma \in \mathfrak{S}_s$ et des matrices inversibles $P_{i,j}$ $(1 \leqslant i \leqslant s,\ j=1,2)$ telles que $P_{i,2}A_{\sigma(i)}P_{i,1}^{-1} = A'_i$ pour tout i.*

2.7. Exercice. *Soient m, n et p trois entiers tels que $0 \leqslant p \leqslant \min(m,n)$. On veut montrer que l'ensemble R_p des matrices de $\mathscr{M}_{n,m}(\mathbb{C})$ de rang p satisfait à la propriété suivante.*

> *Pour A et B quelconques dans R_p, il existe C dans R_p tel que les segments $[AC]$ et $[CB]$ sont dans R_p.*

On dit que R_p est flexé *et que C est un* pivot *pour le couple (A,B).*

1. *Montrer que pour A, B dans R_p, (A,B) peut s'écrire comme somme directe de couples de la forme suivante :* (A_k,B_k), $({}^tA_k,{}^tB_k)$, $\big(\mathrm{I}_k,B(\lambda)\big)$ *avec* $\lambda\neq 0$, $\big(\mathrm{I}_k\oplus A(\infty),B(0)\oplus\mathrm{I}_k\big)$.

   Décomposer tout d'abord (A,B) en une somme directe d'indécomposables de la liste et calculer son rang en fonction de la décomposition. Imposer ensuite que A et B aient même rang.

2. *Montrer qu'il existe un pivot pour chacun de ces couples. Plus précisément :*

   (a) *Les segments* $[A_kB_k]$ *et* $[{}^tA_k\,{}^tB_k]$ *sont contenus dans* R_k.

   (b) *Pour* λ *non nul, le segment* $[\mathrm{I}_kB(\lambda)]$ *est contenu dans* R_k *si* λ *n'est pas un réel négatif.*

   (c) *Pour* λ *strictement négatif et* μ *complexe non réel,* $\mu\mathrm{I}_k$ *est un pivot pour* $\big(\mathrm{I}_k,B(\lambda)\big)$ *dans* R_k.

   (d) *La matrice suivante est un pivot pour* $(\mathrm{I}_k\oplus A(\infty),B(0)\oplus\mathrm{I}_k)$ *dans l'ensemble* R_{2k-1}.

$$C=\begin{pmatrix}0&0&\cdots&0&1\\0&1&\cdots&0&0\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&0\\0&0&\cdots&0&0\end{pmatrix}\in\mathscr{M}_{2k}(\mathbb{C}).$$

3. *Vérifier que l'action de* $\mathrm{GL}_n(\mathbb{C})\times\mathrm{GL}_m(\mathbb{C})$ *envoie un segment de* R_p *vers un segment de* R_p, *puis conclure que* R_p *est flexé.*

Merci à Rached Mneimné pour nous avoir suggéré cet exercice.

3. Problèmes de type sauvage

Voici un autre problème d'algèbre linéaire, très simple à énoncer, extraordinairement compliqué à résoudre (pour simplifier, on dira : impossible) : trouver une forme normale pour un couple d'endomorphismes ou, ce qui revient au même, trouver pour tout entier n une classification des orbites de l'action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathscr{M}_n(\mathbb{K})\times\mathscr{M}_n(\mathbb{K})$ par conjugaison simultanée, c'est-à-dire :

$$g\cdot(A,B)=(gAg^{-1},gBg^{-1}),\quad g\in\mathrm{GL}_n(\mathbb{K}),\ (A,B)\in\mathscr{M}_n(\mathbb{K})\times\mathscr{M}_n(\mathbb{K}).$$

La difficulté du problème a été mise en évidence par Gel'fand et Ponomarev [34]. La remarque de base est la suivante : pour tout entier r, si $a_1,\dots,a_r$ sont des matrices $d\times d$, on construit deux matrices A et B de

taille $N \times N$, où $N = (r+2)d$, en posant :

$$A = \begin{pmatrix} 0 & \mathrm{I}_d & & & & \\ & \ddots & \mathrm{I}_d & & & \\ & & \ddots & & & \\ & & & & \ddots & \mathrm{I}_d \\ & & & & & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & & & & & \\ \mathrm{I}_d & & & & & \\ a_1 & & & & & \\ & a_2 & & & & \\ & & & \ddots & \ddots & \\ & & & a_r & \mathrm{I}_d & 0 \end{pmatrix}.$$

Gel'fand et Ponomarev montrent[7] que si l'espace $\mathbb{K}^d$ ne peut pas se décomposer comme somme directe de deux sous-espaces stables par les a_k, il en est de même de $\mathbb{K}^N$ sous l'action de A et B. Aussi, une classification pour le problème des deux matrices devrait, en quelque sorte, donner une classification *simultanée* pour le problème des r matrices pour *toute* valeur de r. On devrait avoir, au moins, des familles à r paramètres (une valeur des propres de a_k, par exemple) pour tout r. On voit que ce n'est pas simple.

Par ailleurs, on peut montrer qu'en un certain sens, « la théorie n'est pas décidable ». Cela signifie que l'on peut y poser un problème au moins aussi compliqué que le *problème du mot*[8] dans un groupe, c'est-à-dire qu'il n'existe aucun algorithme capable de le résoudre. On peut se dire que si l'on avait une classification raisonnable, on pourrait écrire un algorithme pour résoudre le problème en question.

La surprise suivante, c'est qu'il y a une trichotomie[9] pour les problèmes d'algèbre linéaire :

- problèmes *de type fini* : il n'y a qu'un nombre fini de classes d'indécomposables ; exemples : une application linéaire à changement de base au départ et à l'arrivée, problème des trois sous-espaces ;
- problèmes *de type docile* : en toute dimension, les classes d'indécomposables se répartissent en un nombre fini de familles à un paramètre ; exemples : un endomorphisme linéaire à changement de base près (la matrice de Jordan indécomposable de spectre $\{\lambda\}$), problème des quatre

[7] Ils montrent en fait un peu plus, à savoir que l'espace des morphismes qui commutent aux a_k dans $\mathbb{K}^d$ est isomorphe à l'espace des morphismes qui commutent à A et B dans $\mathbb{K}^N$. Ce n'est pas très difficile une fois que l'on a les formules pour A et B : un joli exercice ?

[8] Le problème du mot est la recherche d'un algorithme qui décide si, dans un groupe présenté par générateurs et relations, deux mots en les générateurs représentent le même élément dans le groupe. Il *n'existe pas* d'algorithme qui permet de résoudre le problème dans cette généralité. (Mais il y en a pour des classes de groupes particulières, comme les groupes abéliens ou les groupes de Coxeter définis à la remarque I-B.13.

[9] C'est grave docteur ?

sous-espaces (quatre droites dans le plan paramétrées par le birapport λ), deux matrices à équivalence simultanée près (familles $(A_k(\lambda), B_k(\lambda))$) ;

- problèmes *de type sauvage* : problème au moins aussi compliqué que le problème des deux endomorphismes ; exemple : problème des cinq sous-espaces, problème des trois endomorphismes...

Pour plus de détails, on renvoie au chapitre IV du livre de David Benson [6] et aux références qu'il contient.

4. Représentations de carquois : introduction

Un carquois est un graphe, *i.e.* la donnée de sommets et de flèches ; représenter un carquois consiste à placer des espaces sur les sommets et des applications linéaires sur les flèches. Pour faire bref, le but de la théorie est de classer les représentations d'un carquois donné modulo l'action naturelle d'un groupe, euh, naturel dans le contexte.

La théorie des carquois soulève un problème général, disons-le, presque métaphysique. Et ce n'est pas une tâche facile que de l'introduire tant les questions qu'elle soulève sont générales et enracinées dans la culture mathématique. On se limitera à deux points de vue.

Pour commencer, on peut résumer presque toute l'algèbre linéaire de licence dans l'étude des représentations de certains carquois simples. En L1, on commence par les représentations du point $\bullet$, c'est-à-dire par la théorie des espaces vectoriels, exemple 4.7. En L1-L2, on s'attaque à la flèche $\bullet \longrightarrow \bullet$, c'est-à-dire aux applications linéaires, exemple 4.8. En L2-L3, cela culmine avec la boucle $\bullet \circlearrowleft$, c'est-à-dire avec les endomorphismes, exemple 4.9. Puisqu'en master, on n'apprend plus rien de vraiment nouveau sur l'algèbre linéaire, la théorie de Gabriel peut être vue comme relevant du programme de L4. (Pas de panique, la réforme n'est pas sortie !)

Le second point de vue est plus ancré dans la géométrie. Nous avons parlé de configurations et de morphismes de configurations. Peut-on donner un sens plus algébrique à cela ? La théorie des représentations, abordée avec le langage des A-modules, permet de relier un problème ancien (la classification des configurations) à des méthodes plus actuelles. En fait, la classification des configurations se ramène à la classification de A-modules pour une algèbre A convenable.

Pour donner un exemple, le fait pour k droites d'être en configuration générale dans un espace de dimension n peut se dire en termes (homologiques) d'*auto-extension* de A-modules. On va ainsi réactualiser notre vision des configurations, et les voir tantôt comme orbites de groupe, tantôt comme

modules sur une algèbre, considérer des adhérences, et même voir ces adhérences de façon purement algébrique. Bref, on raccorde la théorie des configurations à d'autres théories, ce qui permettra d'utiliser des outils plus modernes et plus puissants.

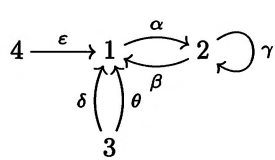
Le point culminant du chapitre sera le théorème de Gabriel, qui décrit les carquois dont les algèbres n'ont qu'un nombre *fini* de représentations indécomposables. Pour cela, il faut rassembler un bon nombre de pièces de puzzle. Pour comprendre ce problème, au départ géométrique, on va utiliser la théorie des A-modules. À ce stade, on peut donner une idée de la chose puisque l'on a su ramener, en II-A, le problème de la classification des endomorphismes au problème, plus algébrique, des modules de type finis sur $\mathbb{K}[X]$. On utilisera également, de façon plus ou moins cachée, de la géométrie algébrique et de l'algèbre homologique. De grands efforts ont été faits pour éviter les catégories ou la géométrie algébrique et mettre ainsi cette élégante théorie à la portée des étudiants de master (motivés) ; c'est parfois au prix de versions moins générales des théorèmes ou de preuves un peu moins naturelles.

4.1. Définition (Carquois). Un *carquois* Q est la donnée d'un ensemble Q_0 (de *sommets*), d'un ensemble Q_1 (de *flèches*) et de deux applications $s : Q_1 \to Q_0$ (source) et $t : Q_1 \to Q_0$ (but ou terminus).

Si, pour une flèche $\alpha \in Q_1$, on a : $s(\alpha) = t(\alpha)$, alors α est appelée *boucle.*

Le carquois Q est dit *fini* siQ_0 et Q_1 le sont. Tous les carquois considérés dans la suite seront supposés finis.

4.2. Exemple. On voit bien comment passer de ces données à un dessin.



Formellement, on a : $Q_0 = \{1,2,3,4\}$, $Q_1 = \{\alpha,\beta,\gamma,\delta,\varepsilon,\theta\}$, $s(\alpha) = 1$, $t(\alpha) = 2$, $s(\beta) = 2$, $t(\beta) = 1$, $s(\gamma) = 2$, $t(\gamma) = 2$, $s(\delta) = 3$, $t(\delta) = 1$, $s(\varepsilon) = 4$, $t(\varepsilon) = 1$, $s(\theta) = 3$, $t(\theta) = 1$.

On fixe dans la suite un carquois fini Q. On va définir comme à l'accoutumée une structure par ses objets et ses morphismes (on l'a souvent fait avec les groupes, les anneaux, les corps...).

4.3. Définition (Représentation d'un carquois). Une *représentation* du carquois Q sur $\mathbb{K}$ est la donnée V d'un $\mathbb{K}$-espace vectoriel de dimension finie V_i pour tout i de Q_0 et d'une application linéaire $V_\alpha : V_{s(\alpha)} \to V_{t(\alpha)}$ pour toute flèche α de Q_1.

Un *morphisme* entre deux représentations de carquois $f : V \to W$ est la donnée d'une famille d'applications linéaires $f_i : V_i \to W_i$ pour i de Q_0 telle que le diagramme

$$\begin{array}{ccc} V_{s(\alpha)} & \xrightarrow{V_\alpha} & V_{t(\alpha)} \\ {\scriptstyle f_{s(\alpha)}}\downarrow & & \downarrow{\scriptstyle f_{t(\alpha)}} \\ W_{s(\alpha)} & \xrightarrow{W_\alpha} & W_{t(\alpha)} \end{array}$$

commute pour toute flèche $\alpha \in Q_1$. Le *morphisme identité* d'une représentation V est la famille $(\mathrm{Id}_{V_i})_{i\in Q_0}$. La composée de $f : V \to W$ avec $g : U \to V$ est la famille $(f_i \circ g_i)_{i\in Q_0}$. Un *isomorphisme* de représentations est un morphisme f qui possède un inverse pour la composition, c'est-à-dire tel que tous les f_i sont inversibles.

On notera $\mathrm{Hom}_{\mathbb{K}Q}(V, W)$ l'espace des morphismes de représentations de V vers W et $\mathrm{End}_{\mathbb{K}Q}(V) = \mathrm{Hom}_{\mathbb{K}Q}(V, V)$.

Soit V une représentation de Q. Une *sous-représentation* de V est déterminée par un sous-espace V'_i de V_i pour chaque sommet i de Q_0, de sorte que l'on ait l'inclusion $V_\alpha(V'_{s(\alpha)}) \subset V'_{t(\alpha)}$ pour toute flèche α de Q_1. Ainsi, V_α induit une application linéaire $V'_\alpha : V'_{s(\alpha)} \to V'_{t'(\alpha)}$ pour chaque α, ce qui définit bien une représentation.

Alors, chaque V_α induit un morphisme $\bar{V}_\alpha : V_{s(\alpha)}/V'_{s(\alpha)} \to V_{t(\alpha)}/V'_{t(\alpha)}$, ce qui permet de définir la *représentation quotient* V/V' comme la famille d'espaces $(V_i/V'_i)_{i\in Q_0}$ munie de la famille de morphismes $\left(\bar{V}_\alpha\right)_{\alpha\in Q_1}$.

On dit que la représentation $V = (V_i)_{i\in Q_0}$ est *irréductible* ou *simple* si elle n'est pas réduite à $\{0\}$ et si ses seules sous-représentations sont $\left(\{0\}\right)_{i\in Q_0}$ et $(V_i)_{i\in Q_0}$.

On définit la *somme directe* $V \oplus W$ de deux représentations V et W du carquois Q de la façon suivante : l'espace associé au sommet i est $(V \oplus W)_i = V_i \oplus W_i$ et l'application linéaire associée à la flèche α est alors dans cette décomposition $(V \oplus W)_\alpha = V_\alpha \oplus W_\alpha$. Une représentation V est dite *indécomposable* si elle n'est pas réduite à $\{0\}$ et s'il n'existe pas de décomposition non triviale de V en somme directe de deux représentations.

4.4. Remarque. Ceux qui connaissent la notion de catégorie (ce qui ne sera pas nécessaire ici) auront reconnu que nous avons défini là la catégorie des représentations du carquois Q sur $\mathbb{K}$.

4.5. Exemple. Pour le carquois $\bullet \longrightarrow \bullet$, on décrit trois représentations : $S_1 : \mathbb{C} \longrightarrow 0$, $P_1 : \mathbb{C} \xrightarrow{\mathrm{Id}} \mathbb{C}$ et $S_2 : 0 \longrightarrow \mathbb{C}$. Elles sont indécomposables : c'est clair pour S_1 et S_2 ; pour P_1, au vu des dimensions, la seule possibilité de décomposition serait que P_1 soit isomorphe à $S_1 \oplus S_2$, alors que $S_1 \oplus S_2 : \mathbb{C} \xrightarrow{0} \mathbb{C}$, et il est facile de vérifier que ce n'est pas le cas. On a des morphismes de représentations $P_1 \to S_1$ et $S_2 \to P_1$ décrits par les diagrammes commutatifs

$$\begin{array}{ccc} P_1 : & \mathbb{C} & \xrightarrow{\mathrm{Id}} \mathbb{C} \\ \downarrow & \downarrow{\scriptstyle \mathrm{Id}} & \downarrow \\ S_1 : & \mathbb{C} & \longrightarrow 0 \end{array} \qquad \begin{array}{ccc} S_2 : & 0 & \xrightarrow{\mathrm{Id}} \mathbb{C} \\ \downarrow & \downarrow & \downarrow{\scriptstyle \mathrm{Id}} \\ P_1 : & \mathbb{C} & \xrightarrow{\mathrm{Id}} \mathbb{C} \end{array}$$

Il n'y a, à multiplication par un scalaire près, que ces morphismes-là : par exemple, on peut voir qu'il n'y a pas de morphisme non nul de S_1 vers P_1 ni, de façon duale, de P_1 vers S_2.

4.6. Problème. Par analogie avec le problème des N-sous-espaces du paragraphe 1, on veut classer, pour un carquois fini Q, toutes les représentations de Q à isomorphisme près. Pour cela, on veut classer toutes ses représentations indécomposables à isomorphisme près.

Le lecteur qui douterait du bien-fondé de ce problème pourra se motiver avec les exemples qui suivent.

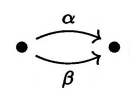
4.7. Exemple. Une représentation du carquois réduit à un sommet $\bullet$ est tout simplement la donnée d'un $\mathbb{K}$-espace vectoriel de dimension finie. Un morphisme entre deux représentations est une application linéaire entre deux espaces. La classification cherchée est tout simplement la classification des espaces à isomorphisme près : la dimension est un invariant total.

4.8. Exemple. Une représentation du carquois $1 \xrightarrow{\alpha} 2$ est la donnée de deux espaces vectoriels de dimension finie et d'une application linéaire de l'un vers l'autre. Un morphisme entre les représentations V et W est la donnée de deux applications linéaires f_i, $i = 1, 2$, de V_i vers W_i telle que $W_\alpha \circ f_1 = f_2 \circ V_\alpha$. L'espace des endomorphismes pour la représentation V est donc $\{(f_1, f_2),\ V_\alpha \circ f_1 = f_2 \circ V_\alpha\} \subset \mathrm{End}(V_1) \oplus \mathrm{End}(V_2)$. La classification cherchée est celle des applications linéaires à changement de base près connue depuis le théorème du rang [H2G2, théorème I-1.3] et un invariant complet est le triplet formé des dimensions des espaces V_1 et V_2 et du rang de l'application V_α.

4.9. Exemple. Une représentation du carquois « boucle » $1 \circlearrowright \alpha$ est la donnée d'un espace vectoriel de dimension finie $V = V_1$ et d'un endomorphisme V_α. Un morphisme entre les représentations V et W est la donnée d'une application linéaire f telle que $W_\alpha \circ f = f \circ V_\alpha$. L'espace des endomorphismes pour la représentation V est donc le commutant de V_α. La classification cherchée est alors la classification des endomorphismes à conjugaison près (autrement dit, la réduction) et un invariant complet est donné par les invariants de similitude, vus dans [H2G2, théorème III-5.7].

4.10. Remarque. On suppose que $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$. Dans ces exemples, les espaces d'endomorphismes de représentations s'identifient aux algèbres de Lie[10] de stabilisateurs pour des actions bien connues. En 4.7, on a l'algèbre de Lie de $\mathrm{GL}_n(\mathbb{K})$; en 4.8, il s'agit de l'algèbre de Lie du stabilisateur d'une application linéaire pour l'action de $\mathrm{GL}_{n_1}(\mathbb{K}) \times \mathrm{GL}_{n_2}(\mathbb{K})$ définie dans [H2G2, proposition I-3.5] ; en 4.9, on reconnaît l'algèbre de Lie du stabilisateur d'un endomorphisme pour l'action de conjugaison.

4.11. Exemple. Soit Q le carquois :



Une représentation de Q est un couple d'espaces vectoriels $V = (E, F)$ et d'un couple d'applications linéaires (V_α, V_β) de E dans F. Un isomorphisme de représentations de V vers V' est un couple d'isomorphismes $(g : E \to E', h : F \to F')$ tels que $h \circ V_\alpha = V'_\alpha \circ g$ et $h \circ V_\beta = V'_\beta \circ g$. On reconnaît la notion d'équivalence. Il en est de même pour la somme directe de couples d'applications linéaires, d'indécomposabilité, etc. Autrement dit, le théorème de Jordan-Kronecker 2.4 décrit les représentations indécomposables du carquois Q.

4.12. Morphismes, version 2

Une façon plus conceptuelle de définir les morphismes entre les représentations V et W est la suivante : on considère les espaces $\bigoplus_{i \in Q_0} \mathrm{Hom}_{\mathbb{K}}(V_i, W_i)$ et $\bigoplus_{\alpha \in Q_1} \mathrm{Hom}_{\mathbb{K}}(V_{s(\alpha)}, W_{t(\alpha)})$ et l'application linéaire φ définie par

$$\begin{array}{rccc} \varphi : & \displaystyle\bigoplus_{i \in Q_0} \mathrm{Hom}_{\mathbb{K}}(V_i, W_i) & \longrightarrow & \bigoplus_{\alpha \in Q_1} \mathrm{Hom}_{\mathbb{K}}(V_{s(\alpha)}, W_{t(\alpha)}) \\ & (f_i)_{i \in Q_0} & \longmapsto & \left(W_\alpha f_{s(\alpha)} - f_{t(\alpha)} V_\alpha\right)_{\alpha \in Q_1}. \end{array}$$

Alors, $(f_i)_{i \in Q_0}$ est un morphisme de représentations si et seulement si pour tout α dans Q_1, on a $W_\alpha f_{s(\alpha)} - f_{t(\alpha)} V_\alpha = 0$, c'est-à-dire si $(f_i)_{i \in Q_0} \in \ker \varphi$.

[10] La notion est définie par exemple dans [H2G2, annexe IX-B]

L'espace $\mathrm{Hom}_{\mathbb{K},Q}(V,W)$ des morphismes de représentations est donc le noyau de φ. Cela nous donne-t-il la dimension $[V,W]^0$ de $\mathrm{Hom}_{\mathbb{K},Q}(V,W)$? Malheureusement non, puisque φ n'est en général pas surjectif. En revanche, si l'on note $[V,W]^1$ la dimension du *conoyau* de φ, c'est-à-dire la dimension du quotient de $\bigoplus_{\alpha\in Q_1}\mathrm{Hom}(V_{s(\alpha)},W_{t(\alpha)})$ par l'image $\mathrm{im}(\varphi)$, la formule du rang donne :

$$\begin{aligned}[V,W]^0-[V,W]^1&=\dim\bigoplus_{i\in Q_0}\mathrm{Hom}_{\mathbb{K}}(V_i,W_i)-\dim\bigoplus_{\alpha\in Q_1}\mathrm{Hom}(V_{s(\alpha)},W_{t(\alpha)})\\&=\sum_{i\in Q_0}\dim V_i\dim W_i-\sum_{\alpha\in Q_1}\dim V_{s(\alpha)}\dim W_{t(\alpha)}.\end{aligned}$$

Cela amène naturellement aux définitions suivantes.

4.13. Définition. Soit Q un carquois et soit V une représentation de Q. On définit le *vecteur de dimension* de V par : $\mathbf{dim}(V)=(\dim V_i)\in\mathbb{N}^{Q_0}$.

La *forme homologique* est la forme bilinéaire $\langle\cdot\,,\cdot\rangle$ définie sur $\mathbb{R}^{Q_0}$ par :

$$\langle x,y\rangle=\sum_{i\in Q_0}x_iy_i-\sum_{\alpha\in Q_1}x_{s(\alpha)}y_{t(\alpha)}\quad(x,y\in\mathbb{R}^{Q_0}).$$

Voici donc un outillage de base pour amorcer l'étude des représentations de carquois et ses invariants :

- le vecteur de dimension $\mathbf{dim}(V)$, qui est un invariant plutôt grossier (avec tout le respect qui lui est dû) ;
- les nombres $[V,W]^0$, $[V,W]^1$, qui sont des objets plus subtils ;
- l'invariant $[V,W]^0-[V,W]^1$, qui est plus simple à comprendre, puisqu'il a le bon goût de se réaliser via une forme bilinéaire réelle — non symétrique, mais ne soyons pas trop gourmands — d'après le corollaire suivant.

4.14. Corollaire. *Avec les notations ci-dessus, on a :*

$$[V,W]^0-[V,W]^1=\big\langle\mathbf{dim}(V),\mathbf{dim}(W)\big\rangle.$$

Démonstration. C'est une réécriture de la formule de la fin du §4.12. □

5. Suites exactes et extensions

On arrive à un point clé de la théorie avec la notion d'extension. C'est par cette notion, riche de divers avatars algébriques et géométriques, que la théorie des carquois va s'ouvrir comme par enchantement.

On commence par un lemme qui découle directement de la définition d'un morphisme de représentations.

5.1. Lemme. *Soient V et W deux représentations d'un carquois Q et soit f un morphisme de V dans W. Alors, pour toute flèche α dans Q_1, V_α envoie* $\ker f_{s(\alpha)}$ *sur* $\ker f_{t(\alpha)}$. *De même, W_α envoie* $\operatorname{im} f_{s(\alpha)}$ *sur* $\operatorname{im} f_{t(\alpha)}$.

5.2. Définition. Le lemme 5.1 permet donc de définir le *noyau* $\ker(f)$ du morphisme f par $\ker(f)_i = \ker(f_i)$ pour tout sommet i et $\ker(f)_\alpha = V_\alpha|_{\ker f_{s(\alpha)}}$ pour toute flèche α.

De même, on peut définir l'*image* $\operatorname{im}(f)$ du morphisme f par $\operatorname{im}(f)_i = \operatorname{im}(f_i)$ pour tout i et $\operatorname{im}(f)_\alpha = W_\alpha|_{\operatorname{im} f_{s(\alpha)}}$ pour tout α.

On dit que la suite de morphismes de représentations

$$0 \longrightarrow V \xrightarrow{\iota} E \xrightarrow{\pi} W \longrightarrow 0$$

est *exacte* si ι est injective ($\ker \iota = 0$), π est surjective ($\operatorname{im} \pi = W$) et si l'on a : $\operatorname{im} \iota = \ker \pi$. On dit alors que E est une *extension* de W par V.

On va donner un moyen de construire des extensions de W par V à l'aide du conoyau de l'application linéaire φ définie en 4.12.

5.3. Définition. Soient V et W deux représentations du carquois Q. On appelle respectivement espace des *cycles* et espace des *bords* pour le couple (W, V) les espaces :

$$Z(W,V) = \bigoplus_{\alpha \in Q_1} \operatorname{Hom}_{\mathbb{K}}\big(W_{s(\alpha)}, V_{t(\alpha)}\big) \text{ et } B(W,V) = \varphi\Big(\bigoplus_{i \in Q_0} \operatorname{Hom}_{\mathbb{K}}(W_i, V_i)\Big),$$

Par construction, on a : $B(W,V) \subset Z(W,V)$. On appelle espace des *extensions* pour (W,V) l'espace :

$$\operatorname{Ext}^1(W,V) = Z(W,V)/B(W,V),$$

On a donc par définition l'égalité

$$\dim \operatorname{Ext}^1(W,V) = [W,V]^1.$$

Pour expliquer cette nouvelle terminologie, on va commencer par construire une extension $E = E_Z$ à partir d'un élément $Z = (Z_\alpha)_{\alpha \in Q_1}$ de $Z(W,V)$ de la manière suivante :

- pour tout sommet i de Q_0, on pose $E_i = V_i \oplus W_i$;
- pour toute flèche α de Q_1, on pose $E_\alpha = V_\alpha \oplus (Z_\alpha + W_\alpha)$ (la somme directe étant liée à la somme directe $E_i = V_i \oplus W_i$).

Cela s'écrit plus agréablement sous forme matricielle. On fixe une base des E_i adaptée à la décomposition. Pour la représentation X, on remplace

l'application linéaire X_α par une matrice x_α notée avec la minuscule correspondante. On obtient :

$$e_\alpha = \begin{pmatrix} v_\alpha & z_\alpha \\ 0 & w_\alpha \end{pmatrix}.$$

La représentation E est une extension de W par V pour l'injection naturelle ι de V dans E et la projection π de E sur W.

On dit, voir l'annexe A.17.3, que deux extensions E et E' de W par V sont *équivalentes* s'il existe un isomorphisme de représentations $f : E \to E'$ tel que le diagramme suivant commute

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \xrightarrow{\iota} & E & \xrightarrow{\pi} & W & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_V} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{Id}_W} & & \\ 0 & \longrightarrow & V & \xrightarrow{\iota'} & E' & \xrightarrow{\pi'} & W & \longrightarrow & 0. \end{array}$$

La proposition suivante éclaire la terminologie en établissant un lien entre classes d'équivalence d'extensions et $\mathrm{Ext}^1(W,V)$. Voir aussi la proposition A.18 pour une interprétation en termes de A-modules.

5.4. Proposition. *Soient W et V deux représentations du carquois Q et soient Z et Z' dans $Z(W,V)$. Les extensions E_Z et $E_{Z'}$ sont équivalentes si et seulement si les classes de Z et de Z' sont égales dans* $\mathrm{Ext}^1(W,V)$.

Démonstration. On suppose que les extensions E_Z et $E_{Z'}$ sont équivalentes, d'où un diagramme commutatif comme ci-dessus avec $E = E_Z$ et $E' = E_{Z'}$. On fixe une base de $(\bigoplus_i V_i)\oplus(\bigoplus_i W_i)$ compatible avec cette décomposition. Écrivons la matrice de f par blocs sous la forme

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

de sorte que la commutation du diagramme avec les injections ι et ι' est équivalente à $a = \mathrm{Id}_V$ et $c = 0$, et que la commutation du diagramme avec les projections π et π' est équivalente à $d = \mathrm{Id}_W$.

Il reste à interpréter le fait que f est un morphisme de représentations. La condition « être un morphisme » s'exprime matriciellement par :

$$\begin{pmatrix} \mathrm{Id}_V & b \\ 0 & \mathrm{Id}_W \end{pmatrix}\begin{pmatrix} v & z \\ 0 & w \end{pmatrix} - \begin{pmatrix} v & z' \\ 0 & w \end{pmatrix}\begin{pmatrix} \mathrm{Id}_V & b \\ 0 & \mathrm{Id}_W \end{pmatrix} = 0,$$

ce qui donne : $z' = z + vb - bw$. Soit $B \in \bigoplus_i \mathrm{Hom}(W_i, V_i)$, B ayant pour matrice b dans la base fixée. Il vient : $Z' = Z + \varphi(B)$, ce qui implique que les classes de Z et de Z' sont égales dans $\mathrm{Ext}^1(W,V)$.

La réciproque est analogue : s'il existe un bord B tel que $Z' = Z + \varphi(B)$, alors on peut construire un isomorphisme de représentations f de E_Z vers $E_{Z'}$ par blocs comme ci-dessus, avec $a = \mathrm{Id}_V$, b est la matrice de B, $c = 0$ et $d = \mathrm{Id}_W$. On vérifie alors que l'on a bien un diagramme commutatif, et donc que les extensions sont bien équivalentes. □

5.5. Définition. Une extension est dite *scindée*[11] si elle est équivalente à l'extension triviale. On dit alors également que la suite exacte correspondante est scindée.

Comme à l'accoutumée (dans les produits semi-directs, etc.), une suite exacte est scindée si et seulement si l'on peut trouver une section à la surjection ou une rétraction à l'injection. Le corollaire suivant est immédiat.

5.6. Corollaire. *On suppose* $[W, V]^1 = 0$. *Alors, toute suite exacte*

$$0 \longrightarrow V \xrightarrow{\iota} E \xrightarrow{\pi} W \longrightarrow 0$$

est scindée. En particulier, E *est isomorphe à* $W \oplus V$.

6. Espace des représentations et actions

On a relié dans les exemples l'étude des classes d'isomorphisme d'un carquois à des actions groupes familières du tome premier. Pour tout vecteur de dimension, on va définir un groupe et une action linéaire sur un espace de représentations, de sorte que le problème de classification se ramène à l'étude des orbites pour cette action. Les nombres $[V, W]^0$ et $[V, W]^1$ définis ci-dessus vont alors s'interpréter en termes d'orbites et de stabilisateurs. Nous voici donc en selle sur notre cheval de bataille !

6.1. Orbite associée à une représentation

On fixe un carquois Q et un vecteur de dimension $\mathbf{d}$ dans $\mathbb{N}^{Q_0}$. En identifiant, pour tout i, l'espace associé au sommet $i \in Q_0$ à $\mathbb{K}^{d_i}$, on voit une $\mathbb{K}$-représentation de vecteur de dimension $\mathbf{d}$ comme un élément de $\bigoplus_{\alpha \in Q_1} \mathrm{Hom}\big(\mathbb{K}^{d_{s(\alpha)}}, \mathbb{K}^{d_{t(\alpha)}}\big)$. Par définition, deux représentations V et W sont isomorphes si et seulement s'il existe $(g_i)_{i \in Q_0}$ dans $\prod_i \mathrm{GL}_{d_i}(\mathbb{K})$ tel que $g_{t(\alpha)} V_\alpha = W_\alpha g_{s(\alpha)}$ pour toute flèche α. La définition ci-dessous permet de relier les classes de représentations du carquois Q avec des orbites pour l'action d'un groupe (de Lie si $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$).

[11] On pourrait préférer le terme *scindable* mais il n'a pas cours.

6.2. Définition. Soit $\mathbf{d} = (d_i) \in \mathbb{N}^{Q_0}$. On appelle *espace des représentations* de vecteur de dimension $\mathbf{d}$ l'espace

$$\mathrm{Rep}_{\mathbf{d}} = \bigoplus_{\alpha \in Q_1} \mathrm{Hom}\big(\mathbb{K}^{d_{s(\alpha)}}, \mathbb{K}^{d_{t(\alpha)}}\big).$$

Cet espace admet une action du groupe $G_{\mathbf{d}} = \prod_{i \in Q_0} \mathrm{GL}_{d_i}(\mathbb{K})$ (dont on notera e le neutre), définie par :

$$(g_i)_{i \in Q_0} \cdot (V_\alpha)_{\alpha \in Q_1} = \big(g_{t(\alpha)} V_\alpha g_{s(\alpha)}^{-1}\big)_{\alpha \in Q_1}.$$

Le lemme suivant est immédiat.

6.3. Lemme. *L'action du groupe $G_{\mathbf{d}}$ sur $\mathrm{Rep}_{\mathbf{d}}$ est bien définie. Deux représentations de $\mathrm{Rep}_{\mathbf{d}}$ sont isomorphes si et seulement si elles sont dans une même $G_{\mathbf{d}}$-orbite.*

6.4. Exemples. Pour le carquois $1 \xrightarrow{\alpha} 2$, on retrouve l'action du groupe $\mathrm{GL}_{d_1}(\mathbb{K}) \times \mathrm{GL}_{d_2}(\mathbb{K})$ sur $\mathrm{Hom}(\mathbb{K}^{d_1}, \mathbb{K}^{d_2})$ donnée par $(g_1, g_2) \cdot A = g_2 A g_1^{-1}$, qui définit les matrices équivalentes. Pour la boucle, on retrouve bien entendu l'action par conjugaison.

L'action de $G_{\mathbf{d}}$ sur $\mathrm{Rep}_{\mathbf{d}}$ va être étudiée à l'aide de la géométrie différentielle, mâtinée d'un soupçon de géométrie algébrique.

On travaille donc ici sur le corps des réels ou des complexes afin d'utiliser l'outillage des groupes de Lie de [H2G2, chapitre IX]. Le groupe $G_{\mathbf{d}}$ est un produit de groupes de Lie : c'est un groupe de Lie dont l'espace tangent en l'identité est :

$$\mathfrak{g}_{\mathbf{d}} = \bigoplus_{i \in Q_0} \mathrm{End}(\mathbb{K}^{d_i}), \quad \text{avec } \dim \mathfrak{g}_{\mathbf{d}} = \sum_{i \in Q_0} d_i^2.$$

Pour toute représentation V de $\mathrm{Rep}_{\mathbf{d}}$, on définit alors l'application différentiable :

$$\psi_V : G_{\mathbf{d}} \longrightarrow \mathrm{Rep}_{\mathbf{d}}, \quad g \longmapsto g \cdot V,$$

où l'action a été définie en 6.2 et dont la différentielle en l'identité e est donnée par :

$$(\mathrm{d}\psi_V)_e : \mathfrak{g}_{\mathbf{d}} \longrightarrow \mathrm{Rep}_{\mathbf{d}}, \quad x \longmapsto \big(x_{t(\alpha)} V_\alpha - V_\alpha x_{s(\alpha)}\big)_{\alpha \in Q_1}.$$

À présent, on se heurte au problème que ψ_V n'est ni une *immersion*, ni une *submersion*. Pas si grave, il s'agit d'une application dont le rang de la différentielle est constant, que l'on appelle aussi *subimmersion*[12].

6.5. Proposition. *La différentielle de ψ_V est de rang constant sur $G_{\mathbf{d}}$.*

[12] Claustrophobes s'abstenir.

Démonstration. Pour tout g dans G, on note L_g la multiplication à gauche par g dans G et ϕ_g l'action de g sur $\mathrm{Rep}_{\mathbf{d}}$. Alors, on a par définition de l'action : $\phi_g \circ \psi_V = \psi_V \circ L_g$. En prenant la différentielle en e on obtient, par linéarité de ϕ_g (resp. L_g) sur $\mathrm{Rep}_{\mathbf{d}}$ (resp. sur $G_{\mathbf{d}} \subset \mathfrak{g}_{\mathbf{d}}$) :

$$\mathbf{d}_V\phi_g \circ \mathbf{d}_e(\psi_V) = \mathbf{d}_g(\psi_V) \circ \mathbf{d}_e(L_g), \quad \text{et donc } \phi_g \circ \mathbf{d}_e(\psi_V) = \mathbf{d}_g(\psi_V) \circ L_g.$$

Comme ϕ_g et L_g sont bijectives, il vient : $\mathbf{d}_g(\psi_V) = \phi_g \circ \mathbf{d}_e(\psi_V) \circ L_g^{-1}$, si bien que les $\mathbf{d}_e(\psi_V)$ ont le même rang. □

Pour une représentation V de Q, on note G_V le stabilisateur de V dans $G_{\mathbf{d}}$.

6.6. Corollaire. *Pour toute représentation V de Q, le groupe G_V est un groupe de Lie et son algèbre de Lie est :*

$$\mathfrak{g}_V = \ker \mathbf{d}_e(\psi_V) = \{f : \forall \alpha \in Q_1,\ f_{t(\alpha)}V_\alpha = V_\alpha f_{s(\alpha)}\} \subset \bigoplus_{i \in Q_0} \mathrm{End}(\mathbb{K}^{d_i}).$$

En particulier, on a : $\dim \mathfrak{g}_V = [V,V]^0$.

Démonstration. On applique le théorème du rang constant, ou plutôt le corollaire C.2 à l'application ψ_V définie sur $G_{\mathbf{d}}$, qui est ouvert dans l'espace vectoriel ambiant. Comme le stabilisateur de V est : $G_V = \psi_V^{-1}(V)$, c'est une sous-variété différentielle de $G_{\mathbf{d}}$ et donc un sous-groupe de Lie[13]. Le calcul de l'algèbre de Lie associée a été fait dans la preuve de 6.5. □

On en déduit par la formule du rang que le rang (constant) de ψ_V est égal à $\dim \mathfrak{g}_{\mathbf{d}} - \dim \mathfrak{g}_V$. On a donc l'inégalité $\dim \mathfrak{g}_{\mathbf{d}} - \dim \mathfrak{g}_V \leqslant \dim \mathrm{Rep}_{\mathbf{d}}$. Mais cette inégalité est déjà établie par un autre procédé :

$$\begin{aligned}\dim \mathrm{Rep}_{\mathbf{d}} - \dim \mathfrak{g}_{\mathbf{d}} + \dim \mathfrak{g}_V &= \sum_{\alpha \in Q_1} d_{s(\alpha)}d_{t(\alpha)} - \sum_{i \in Q_0} d_i^2 + [V,V]^0 \\ &= [V,V]^1 \geqslant 0.\end{aligned}$$

6.7. Remarque. Au bilan, on voit que $[V,V]^0$, qui a été défini à partir d'un noyau, s'interprète maintenant comme la dimension d'un espace tangent au stabilisateur G_V. De même, $[V,V]^1$, qui a été défini comme la dimension d'un conoyau, représente la codimension de l'orbite $G_{\mathbf{d}} \cdot V$ dans $\mathrm{Rep}_{\mathbf{d}}$. On peut se douter qu'il s'agit de la dimension d'un espace normal à l'orbite (mis à part que l'on ne sait pas encore qu'il s'agit d'une sous-variété).

Tout ce dont nous nous servirons dans la suite qui proviendrait de la géométrie différentielle réside dans la proposition suivante.

[13] On aurait pu le déduire du profond théorème de Cartan [60, §3.4], puisque G_V est un sous-groupe fermé, mais pourquoi invoquer les vieux démons qui sommeillent lorsque l'on peut faire autrement ?

6.8. Proposition. *Soit V une représentation telle que $[V,V]^1 > 0$. Alors, l'orbite $G_{\mathbf{d}} \cdot V$ est de mesure nulle pour la mesure de Lebesgue de $\mathrm{Rep}_{\mathbf{d}}$. En particulier, si pour toute représentation V de vecteur de dimension $\mathbf{d}$, on a l'inégalité $[V,V]^1 > 0$, alors le groupe $G_{\mathbf{d}}$ a un nombre infini d'orbites dans $\mathrm{Rep}_{\mathbf{d}}$.*

Démonstration. D'après [47, corollaire V-5.9], un sous-espace vectoriel strictement inclus dans $\mathbb{K}^{n'}$ est de mesure nulle dans $\mathbb{K}^{n'}$, et si f est une fonction lipschitzienne d'un ouvert de $\mathbb{C}^n$ dans $\mathbb{C}^n$, l'image par f d'un ensemble de mesure nulle est encore de mesure nulle. On utilisera tacitement le fait que les applications utilisées dans la suite sont toutes de classe $\mathscr{C}^1$, et donc lipschitziennes sur des compacts.

L'idée est donc de se rappeler que $G_{\mathbf{d}}$ est localement compact et dénombrable à l'infini, voir [H2G2, remarque II-3.4.4], ainsi que l'espace $\mathrm{Rep}_{\mathbf{d}}$ sur lequel il agit. Soient $O \subset G_{\mathbf{d}}$ un voisinage ouvert de l'identité e et $O' \subset \mathrm{Rep}_{\mathbf{d}}$ un voisinage ouvert de V tels que $\psi|_O : O \to O'$ ait la forme donnée par le théorème C.1. On peut choisir O d'adhérence compacte. L'hypothèse $[V,V]^1 > 0$, qui implique que le rang de ψ_V est strictement plus petit que $\dim \mathrm{Rep}_{\mathbf{d}}$ entraîne, par ce qui précède, que l'image $\psi_V(O)$ est de mesure nulle dans $\mathrm{Rep}_{\mathbf{d}}$.

Soit $(K_n)_{n\in\mathbb{N}}$ une famille de compacts tels que l'on ait : $G_{\mathbf{d}} = \bigcup_{n\in\mathbb{N}} K_n$. On peut recouvrir chaque compact K_n par une réunion d'ouverts $\bigcup_{g\in G_{\mathbf{d}}} gO$, dont on peut extraire un recouvrement fini, ce qui fournit en fin de compte un recouvrement de $G_{\mathbf{d}}$ par une réunion dénombrable d'ouverts g_pO ($p \in \mathbb{N}$), avec $g_p \in G_{\mathbf{d}}$ pour tout p.

L'orbite de V est donc $G_{\mathbf{d}} \cdot V = \bigcup_{n\in\mathbb{N}} g_nO \cdot V = \bigcup_{n\in\mathbb{N}} g_n \cdot \psi_V(O)$. Comme les $g_n \cdot \psi_V(O)$ sont de mesure nulle, une réunion dénombrable de ceux-ci est également de mesure nulle.

L'orbite est donc de mesure nulle. La dernière assertion résulte du fait que la réunion finie d'orbites de mesure nulle est encore de mesure nulle. □

6.9. Remarque. Trêve de suspense. On a obtenu ce résultat à moindre frais, l'optique étant l'économie de moyens. Toutefois, à l'aide de résultats un peu plus profonds de géométrie différentielle, on peut obtenir une conclusion beaucoup plus riche et harmonieuse. Tout d'abord, le théorème de Frobenius (voir [47]) permet de trouver des cartes sur le groupe de Lie $G_{\mathbf{d}}$ qui « passent au quotient » et fournissent une structure de variété différentielle sur $G_{\mathbf{d}}/G_V$. L'application différentiable ψ_V passe alors aussi au quotient et induit une immersion $\overline{\psi}_V$ de $G_{\mathbf{d}}/G_V$ dans $\mathrm{Rep}_{\mathbf{d}}$, qui par le théorème d'homéomorphisme, ([H2G2, théorème II-3.4.3]), est un homéomorphisme sur son image. On montre ainsi que $\overline{\psi}_V$ est un plongement, et donc que son image, l'orbite $G_{\mathbf{d}} \cdot V$, est une sous-variété.

6.10. Dégénérescence d'orbites de représentations de carquois

On vient de décomposer un espace en réunion disjointe d'orbites pour l'action continue d'un groupe topologique. Il serait dommage de perdre les bons réflexes acquis dans le tome premier : caractériser les dégénérescences d'orbites.

On rappelle que l'on a fixé un carquois Q et un vecteur de dimension $\mathbf{d}$ de $\mathbb{N}^{Q_0}$. On définit une relation appelée *ordre de dégénérescence* sur les orbites de l'action de $\mathrm{GL}_{\mathbf{d}}$ sur $\mathrm{Rep}_{\mathbf{d}}$ ainsi : pour deux orbites $\mathcal{O}$ et $\mathcal{O}'$, on écrit que $\mathcal{O}' \leqslant_{\mathrm{deg}} \mathcal{O}$ si $\mathcal{O}' \subset \overline{\mathcal{O}}$. Si $\mathcal{O}$ (resp. $\mathcal{O}'$) est l'orbite de la représentation V (resp. V'), on écrira aussi : $V' \leqslant_{\mathrm{deg}} V$. Rappelons que l'on a presque systématiquement étudié cet ordre pour toutes les actions continues importantes qui se sont présentées dans le tome premier : action sur les applications linéaires (proposition I-4.1), action par conjugaison sur les endomorphismes (proposition III-1.6, théorème III-2.7.1 et théorème III-3.3), action à gauche sur les matrices rectangulaire (proposition IV-3.15 et corollaire IV-3.17), action par congruence sur les formes quadratiques (exercice V-1.8)...

D'abord, a-t-on vraiment un ordre[14] ? Autant il est clair que la relation est réflexive et transitive, autant l'antisymétrie pose un problème plus retors. Un résultat standard[15], voir [33, Proposition 2.5.2], sur les actions de groupes en géométrie algébrique permet de montrer que les orbites sont localement fermées, c'est-à-dire ouvertes dans leur adhérence. On a d'ailleurs déjà rencontré des exemples, au [H2G2, corollaire III-2.7.4], ou de la remarque I-4.3, où la situation se présentait. En l'admettant, si l'on a : $\mathcal{O} \leqslant_{\mathrm{deg}} \mathcal{O}'$ et $\mathcal{O}' \leqslant_{\mathrm{deg}} \mathcal{O}$, alors $\mathcal{O}$ et $\mathcal{O}'$ ont la même adhérence où elles sont deux ouverts denses : elles sont donc égales. Mais ce résultat est au-delà de ce que l'on souhaite admettre.

Ensuite, peut-on caractériser cette relation d'ordre de façon algébrique ? combinatoire ? On a fait cette caractérisation dans le tome premier, dans les exemples du rang (proposition I-4.1), des tableaux de Young (théorème III-2.7.1) et des grassmanniennes (proposition IV-3.15).

Nous allons présenter ou illustrer des résultats puissants qui répondent au problème. Nous ne prouverons en fait que la moitié des équivalences, les réciproques restant inaccessibles avec les moyens techniques du moment.

Avant tout, introduisons deux nouvelles relations sur l'ensemble des classes d'isomorphisme de représentations de vecteur de dimension $\mathbf{d}$ donné. On montrera juste après que ce sont des ordres.

---

[14] Contrairement à ce qui se passe dans le langage courant, un ordre n'est pas performatif en mathématiques !

[15] C'est une conséquence du théorème de Chevalley, qui exprime que l'image d'une variété algébrique est *constructible*, c'est-à-dire réunion finie de parties localement fermées.

D'abord, le préordre *hom*. On écrit que $V' \leqslant_{\mathrm{hom}} V$ si, pour toute représentation X du carquois Q, on a : $\dim \mathrm{Hom}_{\mathbb{K}Q}(V,X) \leqslant \dim \mathrm{Hom}_{\mathbb{K}Q}(V',X)$. Cette relation est manifestement réflexive et transitive.

Ensuite, on définit le préordre *ext* ainsi. On écrit $E' \leqslant_{\mathrm{ext-el}} E$ s'il existe une suite exacte

$$0 \longrightarrow V \longrightarrow E \longrightarrow W \longrightarrow 0$$

telle que $E' \simeq V \oplus W$. On écrit $V' \leqslant_{\mathrm{ext}} V$ s'il existe une suite finie $V' = V_0, V_1, \ldots, V_r = V$ telle que $V_i \leqslant_{\mathrm{ext-el}} V_{i+1}$ pour tout $i \leqslant r-1$. La relation $\leqslant_{\mathrm{ext}}$ est réflexive car on a une suite exacte $0 \to 0 \to E \to E \to 0$ et $E \simeq E \oplus 0$. Elle est transitive par construction.

6.11. Proposition. *Les relations $\leqslant_{\mathrm{ext}}$, $\leqslant_{\mathrm{deg}}$ et $\leqslant_{\mathrm{hom}}$ sont des relations d'ordre sur l'ensemble des classes d'isomorphismes de représentations de vecteur de dimension* $\mathbf{d}$.

De plus, pour V et V' représentations de vecteur de dimension $\mathbf{d}$, *on a :*

$$V' \leqslant_{\mathrm{ext}} V \implies V' \leqslant_{\mathrm{deg}} V \implies V' \leqslant_{\mathrm{hom}} V.$$

Démonstration. Dans la preuve, on identifiera l'espace d'une représentation V avec la somme directe des V_i. Les applications linéaires V_α deviennent ainsi des endomorphismes de $V = \bigoplus_{i \in Q_0} V_i$.

Les trois relations étant réflexives et transitives, il ne reste qu'à prouver l'antisymétrie. On va montrer l'antisymétrie de $\leqslant_{\mathrm{hom}}$, puis les implications de la deuxième assertion. L'antisymétrie de $\leqslant_{\mathrm{ext}}$ et $\leqslant_{\mathrm{deg}}$ en résulte aussitôt.

Pour l'antisymétrie de $\leqslant_{\mathrm{hom}}$, on fixe deux représentations V et W de même vecteur de dimension telles que $V \leqslant_{\mathrm{hom}} W$ et $W \leqslant_{\mathrm{hom}} V$, c'est-à-dire que l'on a, pour toute représentation X :

$$\dim \mathrm{Hom}_{\mathbb{K}Q}(V,X) = \dim \mathrm{Hom}_{\mathbb{K}Q}(W,X).$$

On veut montrer $V \simeq W$. Si $V = 0$, alors $W = 0$ aussi puisqu'elle admet même vecteur de dimension, par hypothèse. On considère l'espace vectoriel $\mathrm{Hom}_{\mathbb{K}Q}(V,W)$ et $(\phi_k)_{1 \leqslant k \leqslant n}$ une base de cet espace. Soit $\phi : V^n \to W$ l'application définie par : $\phi(v_1, \ldots, v_n) = \phi_1(v_1) + \cdots + \phi_n(v_n)$.

Soit K le noyau de ϕ, de sorte que l'on a la suite exacte

$$0 \longrightarrow K \xrightarrow{\kappa} V^n \xrightarrow{\phi} W.$$

Par construction, tout morphisme f de V dans W s'écrit $f = \sum_{i=1}^n \lambda_i \phi_i$, ce qui donne une factorisation $\phi \circ g = f$, avec $g(v) = (\lambda_i v)_{1 \leqslant i \leqslant n} \in V^n$.

Ainsi, $\phi\circ?$ est une surjection dans la suite

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{K}Q}(V,K) \xrightarrow{\kappa\circ?} \mathrm{Hom}_{\mathbb{K}Q}(V,V^n) \xrightarrow{\phi\circ?} \mathrm{Hom}_{\mathbb{K}Q}(V,W) \longrightarrow 0.$$

On voit facilement que la suite est alors exacte. De plus, la suite

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{K}Q}(W,K) \xrightarrow{\kappa\circ?} \mathrm{Hom}_{\mathbb{K}Q}(W,V^n) \xrightarrow{\phi\circ?} \mathrm{Hom}_{\mathbb{K}Q}(W,W) \longrightarrow 0$$

est exacte. En effet, la seule difficulté est la surjectivité de $\phi\circ?$, mais cela résulte du fait que la suite précédente était exacte et de l'égalité des dimensions entre $\mathrm{Hom}_{\mathbb{K}Q}(V,X)$ et $\mathrm{Hom}_{\mathbb{K}Q}(W,X)$ pour $X = K$, V^n et W.

En particulier, Id_W a un antécédent σ par $\phi\circ?$, ce qui revient à dire que σ est une section de ϕ qui est un morphisme de représentations. En conclusion, l'application ϕ est surjective et W est un facteur direct de V^n.

De même, par symétrie, V est facteur direct de W^m. Par unicité de la décomposition en indécomposables donnée par le corollaire A.16, cela veut dire que tout indécomposable de la décomposition de V est aussi dans la décomposition de W, et inversement.

Par récurrence sur le nombre d'indécomposables, on en déduit que V et W sont isomorphes. En effet, si $V = I \oplus V'$ avec I indécomposable, alors $W = I \oplus W'$ pour W' convenable et l'on a, pour toute représentation X :

$$\begin{aligned}\dim \mathrm{Hom}_{\mathbb{K}Q}(V',X) &= \dim \mathrm{Hom}_{\mathbb{K}Q}(V,X) - \dim \mathrm{Hom}_{\mathbb{K}Q}(I,X)\\ &= \dim \mathrm{Hom}_{\mathbb{K}Q}(W,X) - \dim \mathrm{Hom}_{\mathbb{K}Q}(I,X)\\ &= \dim \mathrm{Hom}_{\mathbb{K}Q}(W',X)\,;\end{aligned}$$

par récurrence, V' et W' sont isomorphes, donc V et W le sont.

Reste donc à montrer les deux implications. Pour la première, soit E une extension de W par V ; en reprenant les notations du paragraphe précédent, la structure de E est donnée matriciellement sous la forme :

$$e_\alpha = \begin{pmatrix} v_\alpha & z_\alpha \\ 0 & w_\alpha \end{pmatrix}.$$

Soit alors, pour tout λ non nul, l'extension E_λ décrite par :

$$e_\alpha^\lambda = \begin{pmatrix} v_\alpha & \lambda z_\alpha \\ 0 & w_\alpha \end{pmatrix}.$$

L'application linéaire de E dans E_λ donnée par la matrice

$$p_\lambda = \begin{pmatrix} \mathrm{Id}_V & 0 \\ 0 & \lambda^{-1}\mathrm{Id}_W \end{pmatrix}$$

est un isomorphisme de représentations puisque $p_\lambda e_\alpha = e_\alpha^\lambda p_\lambda$.

Il en résulte que E est isomorphe à E_λ. Or, quand λ tend vers 0, E_λ converge vers $V \oplus W$ dans l'espace $\mathrm{Rep}_{\mathbf{d}}$. On a donc : $V \oplus W \leqslant_{\mathrm{deg}} E$.

Pour la seconde implication, il suffit de voir que $\mathrm{Hom}_{\mathbb{K}Q}(V, X)$ est le noyau de l'application φ définie en 4.12 (en remplaçant W par X). Notons-la $\varphi = \varphi_V$. Lorsque V tend vers V' par dégénérescence dans $\mathrm{Rep}_{\mathbf{d}}$, la dimension du noyau de φ_V ne peut qu'augmenter, par semi-continuité inférieure du rang — voir [H2G2, corollaire I-4.5]. Ainsi, on a : $V' \leqslant_{\mathrm{hom}} V$. □

6.12. Remarque. Avec un peu de géométrie algébrique, on montre plus facilement que $\leqslant_{\mathrm{deg}}$ est antisymétrique. Dans ce cadre, le théorème de Chevalley et une propriété d'irréductibilité montrent qu'une orbite est un ouvert dense dans son adhérence et donc que deux orbites possédant la même adhérence sont égales.

6.13. Exemple. Pour le carquois A_2 de l'exemple 4.5 dont on reprend les notations, on a une suite exacte

$$0 \longrightarrow S_2 \longrightarrow P_1 \longrightarrow S_1 \longrightarrow 0,$$

et il vient donc : $S_1 \oplus S_2 \leqslant_{\mathrm{deg}} P_1$. En fait, cette relation engendre l'ordre de dégénérescence pour le carquois A_2. Par exemple, en dimension (n, m), une application linéaire de rang k est dans l'orbite de $P_1^k \oplus S_1^{n-k} \oplus S_2^{m-k}$. Ce dernier dégénère sur $P_1^{k-i} \oplus S_1^{n-k+i} \oplus S_2^{m-k+i}$, pour tout $i \leqslant k$ et l'on reconnaît ainsi [H2G2, corollaire I-4.5] sur de la semi-continuité inférieure du rang.

6.14. Exemple. Attention : ne pas se fier à A_2 pour comprendre l'ordre de dégénérescence ! L'ordre n'est en général pas engendré par la dégénérescence des indécomposables, pris un par un. Par exemple, dans le cas du carquois de type A_3 donné par $\bullet \longrightarrow \bullet \longleftarrow \bullet$, on a les indécomposables P_1, P_3, S_2, I_2 de vecteurs de dimension respectives $(1,1,0)$, $(0,1,1)$, $(0,1,0)$, $(1,1,1)$. On vérifie que l'on a une suite exacte

$$0 \longrightarrow S_2 \longrightarrow P_1 \oplus P_3 \longrightarrow I_2 \longrightarrow 0.$$

(Jeu : deviner ce que sont les flèches en s'inspirant de l'exemple 4.5.)

6.15. Remarque. Les deux réciproques des implications de la proposition 6.11 sont fausses en général. Elles sont prouvées avec adresse et élégance dans des cas particuliers, par exemple pour des carquois de type Dynkin ou Dynkin étendu, par Klaus Bongartz dans [8].

7. Lemme de Ringel et théorème de Gabriel

Nous voici rendus au théorème de Gabriel, qui met en exergue les ubiquitaires diagrammes de Dynkin. Sa preuve, qui a été relativement simplifiée par rapport à l'originale, utilise tout de même le difficile lemme de Ringel. On pourra trouver étonnant, voire incroyable, d'arriver à obtenir, dans une problématique aussi générale que celle des représentations de carquois, un quelconque résultat de classification. Et pourtant...

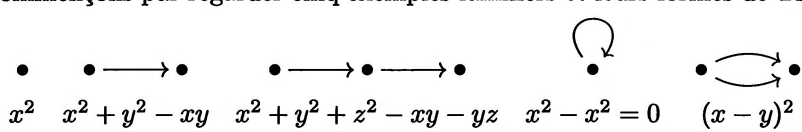
7.1. Forme de Tits définie positive et lemme de Ringel

On revient à présent sur la forme bilinéaire « homologique » $\langle \cdot , \cdot \rangle$ associée au carquois Q. Nous avons dit qu'elle n'était en général pas symétrique, mais nous pouvons toutefois lui associer une forme quadratique. La forme

$$q(\mathbf{d}) = \langle \mathbf{d}, \mathbf{d} \rangle = \sum_{i \in Q_0} d_i^2 - \sum_{\alpha \in Q_1} d_{s(\alpha)} d_{t(\alpha)}$$

sur $\mathbb{R}^{Q_0}$ est appelée *forme de Tits*. Nous allons voir que l'étude de cette forme quadratique est cruciale pour le problème de classification des représentations à isomorphisme près.

Commençons par regarder cinq exemples familiers et leurs formes de Tits :



x^2 $\quad x^2+y^2-xy$ $\quad x^2+y^2+z^2-xy-yz$ $\quad x^2-x^2=0$ $\quad (x-y)^2$

Les cinq formes sont positives et les trois premières sont définies positives. On comprend rapidement, en considérant le carquois à deux sommets et n flèches, dont la forme de Tits associée est x^2+y^2-nxy que la complexité du problème posé grandit lorsque q devient davantage « négative ». Amusant : la forme de Tits ne voit pas le sens des flèches, ce qui suggère que la complexité du problème ne dépend que du graphe non orienté sous-jacent.

Nous commençons avec le redoutable lemme de Ringel, qui donne une conséquence assez inattendue de la positivité de la forme de Tits. Sa preuve, qui force l'admiration, montre un bel exemple d'utilisation des techniques de *pullback* (tirée en arrière) et de *pushforward* (poussée en avant), qui sont expliquées en annexe A.17.

7.2. Théorème (Lemme de Ringel). *On suppose $\mathbb{K} = \mathbb{C}$. Soit Q un carquois dont la forme de Tits est définie positive, voir l'annexe B. Alors, pour toute représentation indécomposable X de Q, les endomorphismes de X sont réduits aux homothéties.*

Démonstration. Dans la preuve, on considérera encore la représentation X comme un espace total $\bigoplus_{i\in Q} X_i$. Les X_α ($\alpha \in Q_1$) pourront alors être considérés comme des endomorphismes de cet espace. De même, un endomorphisme f de la représentation X pourra être vu comme un endomorphisme de l'espace total.

On procède par récurrence sur $\dim X$.

Rappelons que tout endomorphisme d'indécomposable se décompose en une somme d'une homothétie et un endomorphisme nilpotent : c'est un avatar du *lemme de Fitting* A.13. Pour montrer le lemme de Ringel, il suffit donc de montrer que tout endomorphisme nilpotent de X est nul.

Procédant par l'absurde, on suppose que g est un endomorphisme nilpotent de X non nul et l'on choisit g tel que $\dim \operatorname{im}(g)$ est minimal.

Soit n minimal tel que $g^n = 0$. Si $n > 2$, alors g^2 est nilpotent non nul et on sait[16] que $\dim \operatorname{im}(g^2) < \dim \operatorname{im}(g)$: cela contrevient au choix de g donc $n = 2$. Par suite, on a : $\operatorname{im} g \subset \ker g \subsetneq X$. On pose $K = \ker g$ et $I = \operatorname{im} g$. Comme $g^2 = 0$, on a une suite exacte

$$0 \longrightarrow K \longrightarrow X \xrightarrow{g} I \longrightarrow 0. \qquad (\S)$$

On a constaté au lemme 5.1 que $\ker g$ et $\operatorname{im} g$ pouvaient être vus comme des sous-représentations de X. On décompose $K = \ker g = \bigoplus_j K_j$ en somme de représentations indécomposables. Pour tout j, soit π_j la projection de K sur K_j selon cette décomposition. On fixe un indice j tel que $\pi_j|_{\operatorname{im} g}$ soit non nulle — il en existe, sans quoi l'image $\operatorname{im} g$ serait nulle.

Montrons que $\iota = \pi_j|_{\operatorname{im} g}$ est injective. En effet, sinon, on aurait d'une part :

$$0 < \dim \operatorname{im}(\pi_j \circ g) = \dim \operatorname{im}(g) - \dim \ker\bigl(\pi_j|_{\operatorname{im} g}\bigr) < \dim \operatorname{im} g,$$

alors que d'autre part, on a : $(\pi_j \circ g)^2 = 0$ (g s'annule sur K_j !) ; cela contredirait la condition de minimalité de g.

On a donc un morphisme injectif de représentations $\iota : \operatorname{im}(g) = I \hookrightarrow K_j$. Prenons donc la *poussée en avant* de la suite exacte (§) induit par π_j, (annexe A.17). On obtient un diagramme dont les lignes sont exactes :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \xrightarrow{i_X} & X & \xrightarrow{g} & I & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_j} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle \mathrm{Id}_I} & & \\
0 & \longrightarrow & K_j & \xrightarrow{i_Y} & Y & \longrightarrow & I & \longrightarrow & 0.
\end{array}$$

Si la suite du bas était scindée, le morphisme i_Y aurait un inverse à gauche

[16] En effet, la suite des dimensions des noyaux itérés *s'essouffle*, dans la terminologie de [59] ou du tome premier.

(rétraction) r_Y. Et, comme π_j a un inverse à droite (section) s_j, on aurait :

$$(r_Y \circ p) \circ (i_X \circ s_j) = r_Y \circ (p \circ i_X \circ s_j) = r_Y \circ i_Y = \mathrm{Id}_{K_j}.$$

L'injection $i_X \circ s_j$ de K_j dans X aurait donc une rétraction $r_Y \circ p$ et ainsi, la représentation K_j serait facteur direct de X, ce qui est impossible car X est indécomposable. On obtient donc, par le corollaire 5.6, l'inégalité $[I, K_j]^1 \geqslant 1$.

On va maintenant en déduire l'inégalité $[K_j, K_j]^1 \geqslant 1$[17]. Le morphisme injectif ι permet de voir I comme une sous-représentation de K_j. Cette injection induit un morphisme naturel $\zeta(\iota, K_j)$ de $Z(K_j, K_j)$ dans $Z(I, K_j)$, via la composition à droite par ι. Ce dernier est surjectif : pour le voir, il suffit de choisir un supplémentaire, à chaque sommet i du carquois, de I_i dans $(K_j)_i$. Un morphisme dans $Z(I, K_j)$ se prolonge en un morphisme dans $Z(K_j, K_j)$ tel que, pour chaque α dans Q_1, les flèches sont nulles sur les supplémentaires construits.

Or, comme ι est un morphisme de représentations, on voit que $\zeta(\iota, K_j)$ envoie $B(K_j, K_j)$ dans $B(I, K_j)$, d'où, par passage au quotient, un morphisme (qui reste surjectif !) de $\mathrm{Ext}^1(K_j, K_j)$ dans $\mathrm{Ext}^1(I, K_j)$. On obtient bien $[K_j, K_j]^1 \geqslant 1$ comme annoncé.

Or, K_j est indécomposable et strictement inclus dans X, on peut lui appliquer l'hypothèse de récurrence : $[K_j, K_j]^0 = 1$. Il vient : $q(\dim K_j) = [K_j, K_j]^0 - [K_j, K_j]^1 \leqslant 0$, ce qui est absurde vu que K_j est non nul et que q est définie positive. □

On peut voir dans l'exercice qui suit à quel point le résultat est faux pour la boucle, dont la forme de Tits est nulle.

7.3. Exercice. *On considère la représentation de la boucle donnée par l'endomorphisme $j : \mathbb{C}^n \to \mathbb{C}^n$, où la matrice de j dans la base canonique de $\mathbb{C}^n$ est la matrice de Jordan indécomposable*

$$J = \begin{pmatrix} 0 & & & 0 \\ 1 & 0 & & \\ & \ddots & 0 & \\ 0 & & 1 & 0 \end{pmatrix}.$$

1. *Montrer que la représentation est indécomposable.*

   Il faut montrer que $\mathbb{C}^n$ n'est pas somme directe de sous-espaces stables. Mais l'on connaît les sous-espaces stables...

[17] Pour ceux que cela peut éclairer, c'est juste par annulation de la cohomologie en degré 2.

2. *Montrer cependant que l'algèbre des endomorphismes de cette représentation contient des nilpotents non nuls.*

   On sait que cette algèbre est l'algèbre des endomorphismes qui commutent avec J. On y trouve J...

Notons toutefois que le lemme de Fitting, version corollaire A.13, est bien respecté : le commutant de J est, d'après la proposition II-2.2, l'algèbre des polynômes en J, et un tel polynôme se décompose en une homothétie (le terme de degré 0 du polynôme) et un élément nilpotent (la somme des autres termes). Cela traduit bien l'indécomposabilité de la représentation.

7.4. Forme de Tits et théorème de Gabriel

Si le théorème de Gabriel est le point culminant de ce chapitre, il faut savoir qu'il s'agit du camp de base de belles théories très actuelles (groupes quantiques et bases canoniques, algèbres de Hall, algèbres amassées...) et qu'il se situe en lien direct avec la théorie de McKay, dont les origines seront dignement passées en revue à la fin du livre. Le théorème de Gabriel est pourtant un théorème dont les hypothèses sont assez restrictives (même la boucle n'arrive pas à rentrer dans leur cadre!), puisqu'il exige que la forme de Tits soit définie positive, voir l'annexe B pour la classification de tels carquois. Mais la démarche reste toutefois fondamentale. Il est bon de savoir que le théorème de Gabriel se généralise en un théorème dû à Kac pour tout carquois fini, théorème largement hors de portée dans le cadre du présent ouvrage mais dont nous dirons deux mots par la suite.

7.5. Définition. On suppose que Q est un carquois fini dont la forme de Tits associée est définie positive. On appelle, pour des raisons qui échappent au contenu de l'ouvrage, *racine positive* un élément de l'ensemble :

$$\Phi^+ = \left\{\mathbf{d} \in \mathbb{N}^{Q_0},\ q(\mathbf{d}) = 1\right\}.$$

7.6. Lemme. *L'ensemble Φ^+ des racines positives d'un carquois dont la forme de Tits est définie positive est fini.*

Démonstration. Comme la forme quadratique q est définie positive, c'est un produit scalaire euclidien, dont la « sphère-unité » $\{\mathbf{d}\in\mathbb{R}^{Q_0},\ q(\mathbf{d})=1\}$ est un ellipsoïde compact. Donc Φ^+ est fini, comme intersection du l'ensemble discret $\mathbb{N}^{Q_0}$ et d'un compact. (Si Φ^+ était infini, on pourrait trouver une suite dans Φ^+ sans point d'accumulation.) □

Nous sommes enchantés de présenter et de montrer le fameux *théorème de Gabriel.* En réalité, le plus gros du travail a déjà été fait en amont.

7.7. Théorème (Gabriel). *Soit Q un carquois fini. Alors, les conditions suivantes sont équivalentes.*

(1) *La forme de Tits associée à Q est définie positive.*

(2) *Il n'existe qu'un nombre fini de représentations indécomposables à isomorphisme près.*

Si cette condition est satisfaite, alors l'application qui à une représentation V, associe son vecteur de dimension $\mathbf{dim}(V)$ établit une bijection entre les classes de représentations indécomposables de Q et l'ensemble des racines positives Φ^+.

Démonstration. « (2) $\Rightarrow$ (1) » On suppose que q n'est pas définie positive. Montrons tout d'abord qu'il existe un vecteur de dimension $\mathbf{d} \in \mathbb{N}^{Q_0}$ non nul tel que $q(\mathbf{d}) \leqslant 0$. Si q n'est pas positive et que $\mathbb{Q}^{Q_0}$ est dense dans $\mathbb{R}^{Q_0}$, il existe $r \in \mathbb{Q}^{Q_0}$ tel que $q(r) < 0$. Si q est positive non définie, alors q possède un noyau qui est un $\mathbb{R}$-sous-espace vectoriel de dimension $k > 0$. Mais comme q est une forme à coefficients rationnels, son noyau restreint à $\mathbb{Q}^{Q_0}$ est un sous-espace de même dimension k sur $\mathbb{Q}$, puisque c'est le noyau de la matrice de q. Il existe donc $r \in \mathbb{Q}^{Q_0}$ non nul tel que $q(r) = 0$. Dans les deux cas, on trouve un élément $r = (r_i)$ non nul de $\mathbb{Q}^{Q_0}$ tel que $q(r) \leqslant 0$. Comme q est homogène, on peut choisir r dans $\mathbb{Z}^{Q_0}$. Posons $\mathbf{d} = \big(|r_i|\big)_{i \in Q_0} \in \mathbb{N}^{Q_0}$. L'inégalité $-|a||b| \leqslant ab$ donne facilement : $q(\mathbf{d}) \leqslant q(r) \leqslant 0$. On va désormais travailler dans l'espace de représentation $\mathrm{Rep}_{\mathbf{d}}$. Soit V une représentation de vecteur de dimension $\mathbf{d}$. Par construction, on a : $[V,V]^1 = [V,V]^0 - q(\mathbf{d})$, donc $[V,V]^1 \geqslant 1 - q(\mathbf{d}) > 0$, car l'algèbre des endomorphismes de V contient la droite des homothéties. On conclut par la proposition 6.8 qu'il y a une infinité d'orbites de représentations de vecteur de dimension $\mathbf{d}$.

S'il y avait un nombre fini de classes d'indécomposables — disons k classes — le nombre de décompositions possibles en indécomposables, à isomorphisme près, pour une représentation de vecteur de dimension $\mathbf{d}$ serait borné — au pire, par $k^{\sum_i d_i}$. Donc, il y aurait un nombre fini d'orbites, ce qui est absurde. Il existe donc un nombre infini d'indécomposables.

« (1) $\Rightarrow$ (2) » On suppose que q est définie positive. Par le lemme de Ringel, si X est indécomposable, alors $[X,X]^0 = 1$. Or, pour $\mathbf{d} = \mathbf{dim}\, X$, on a :

$$0 \leqslant [X,X]^1 = [X,X]^0 - q(\mathbf{d}) = 1 - q(\mathbf{d}) \leqslant 0.$$

Il vient : $q(\mathbf{d}) = 1$, c'est-à-dire que $\mathbf{d}$ est une racine positive. De plus, par la proposition 6.5, le rang (constant) de la différentielle de φ_X est égal à $\dim \mathrm{Rep}_{\mathbf{d}} - [X,X]^1 = \dim \mathrm{Rep}_{\mathbf{d}}$. Par le théorème C.1 (ici φ_V est une submersion), l'orbite $G_{\mathbf{d}} \cdot X$ de X contient un ouvert de $\mathrm{Rep}_{\mathbf{d}}$ et par le principe de translation, l'orbite est ouverte dans $\mathrm{Rep}_{\mathbf{d}}$.

On introduit donc l'application **dim** qui envoie une classe d'isomorphisme de représentation indécomposable sur son vecteur de dimension. On veut montrer que **dim** est injective et que son image est exactement l'ensemble des racines positives, Φ^+.
Soient X_1 et X_2 indécomposables ; on vient de voir que les orbites $G_{\mathbf{d}} \cdot X_1$ et $G_{\mathbf{d}} \cdot X_2$ sont ouvertes dans $\mathrm{Rep}_{\mathbf{d}}$. Alors, d'après [33, Proposition 1.4.15], ces orbites sont denses dans $\mathrm{Rep}_{\mathbf{d}}$. Or, comme deux ouverts denses s'intersectent, ces deux orbites ont un point commun et sont donc égales. Nous avons montré que X_1 est isomorphe à X_2, autrement dit, que l'application **dim** est injective.
Avant d'attaquer la surjectivité, notons que le nombre de classes d'indécomposables est fini, puisqu'il s'injecte dans l'ensemble fini Φ^+.
Maintenant, soit $\mathbf{d}$ une racine positive. Comme il n'y a qu'un nombre fini de classes d'indécomposables, il n'y a qu'un nombre fini de classes de représentations de vecteur de dimension $\mathbf{d}$. Donc, $\mathrm{Rep}_{\mathbf{d}}$ est la réunion d'un nombre fini d'orbites pour l'action de $G_{\mathbf{d}}$. Soient $X_1, \ldots, X_k$ des représentants de ces orbites. Si pour tout k, on avait : $[X_k, X_k]^1 > 0$, alors, par la proposition 6.8, chaque orbite $G_{\mathbf{d}} \cdot X_k$ serait de mesure nulle et donc $\mathrm{Rep}_{\mathbf{d}}$ serait de mesure nulle, ce qui est absurde. Il existe donc X tel que $[X, X]^1 = 0$. Comme $\mathbf{d}$ est une racine, on obtient : $[X, X]^0 = q(\mathbf{d}) + [X, X]^1 = 1$. Si X était décomposable, on aurait une décomposition non triviale $X = X_1 \oplus X_2$ et les projections sur $X_i \subset X$ fourniraient deux endomorphismes indépendants de X. C'est impossible, de sorte que X est indécomposable et que **dim** est surjective. □

Dans la preuve qui précède, nous avons dû faire appel à une aide extérieure[18] pour la densité des orbites. Disons vaguement que les orbites qui contiennent un ouvert non vide sont denses car les morphismes en présence sont *algébriques*. Pour avoir une idée sommaire de la façon dont les choses marchent, il est instructif de regarder la preuve du corollaire D.5 : il joue là le rôle d'une ampoule à économie d'énergie pour éclairer ce passage obscur.

7.8. Corollaire. *Les carquois n'ayant qu'un nombre fini de représentations indécomposables sont les diagrammes de Dynkin (définition B.1).*

Démonstration. C'est la conjonction du théorème de Gabriel et du théorème B.2, qui décrit les carquois dont la forme de Tits est définie positive. □

On dit parfois qu'un carquois est *de type (de représentation) fini* s'il ne possède qu'un nombre fini de représentations. On reprend à présent quelques exemples qui illustrent le théorème de Gabriel. Rappelons que les racines ne dépendent que de la forme de Tits, et pas de l'orientation du carquois.

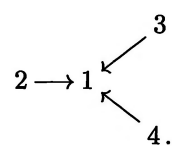
[18] Joker : on a le droit d'appeler un ami.

7.9. Exemple. Pour le sommet sans flèche •, la forme de Tits est x^2 et la seule racine positive est 1. Tout espace vectoriel de type fini est donc une somme directe de copies d'un unique indécomposable. C'est une façon un peu sophistiquée de dire que deux espaces sont isomorphes si et seulement s'ils ont la même dimension.

7.10. Exemple. Pour le carquois $1 \longrightarrow 2$, la forme de Tits est $x_1^2 - x_1x_2 + x_2^2$ et les racines sont $(1,0)$, $(1,1)$, $(0,1)$. On retrouve le fait que toute représentation du carquois se décompose de façon unique en somme directe de $\mathbb{C} \longrightarrow 0$, $\mathbb{C} \xrightarrow{\mathrm{Id}} \mathbb{C}$ et $0 \longrightarrow \mathbb{C}$. Autrement dit, une fois fixées les dimensions des espaces de départ et d'arrivée, une application linéaire est, à changement de base près, caractérisée par son rang : c'est un nouvel avatar du théorème du rang !

7.11. Exemple. Pour le carquois $1 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3$, la forme de Tits est $x_1^2+x_2^2+x_3^2-x_1x_2-x_1x_3-x_2x_3$ et les racines sont $(1,0,0)$, $(1,1,0)$, $(1,1,1)$, $(0,1,0)$, $(0,1,1)$ et $(0,0,1)$. C'est un exercice intéressant de retrouver cette classification à partir du théorème de Jordan, partant du constat que $V_\alpha + V_\beta$ est un endomorphisme nilpotent de $V_1 \oplus V_2 \oplus V_3$.

7.12. Exemple. Étudions de même le carquois suivant, appelé D_4 :



La forme de Tits est $x_1^2+x_2^2+x_3^2+x_4^2-x_1(x_2+x_3+x_4)$. Les racines sont :

$$(2,1,1,1),\ (1,1,1,1),\ (1,1,1,0),\ (1,1,0,1),\ (1,0,1,1),\ (1,1,0,0),$$
$$(1,0,0,0),\ (1,0,0,1),\ (1,0,1,0),\ (0,1,0,0),\ (0,0,1,0),\ (0,0,0,1).$$

Les neuf premières racines correspondent aux représentations indécomposables où les flèches sont injectives : elles sont en bijection avec les configurations de la proposition 1.6. Les trois dernières racines correspondent aux représentations où les flèches ne sont pas injectives. On interprète ainsi les sommets atteints par des pointillés dans le diagramme (AR) du §1.5.

7.13. Mise en garde. Malgré les exemples précédents, la donnée du vecteur dimension des indécomposables ne caractérise pas, en général, une représentation, c'est-à-dire les applications linéaires V_α à associer à chaque flèche α. Par unicité de la représentation indécomposable associée à un vecteur de dimension donnée, et la densité de l'orbite correspondante, on peut parfois deviner une forme normale pour les V_α. Par exemple, une représentation indécomposable pour D_4 de dimension $(2,1,1,1)$ correspond

forcément à trois droites en position générale dans le plan. En revanche, pour les carquois de type E (définition B.1), il faut des techniques constructives, voir [6].

7.14. Remarque. Le théorème de Gabriel introduit au *théorème de Kac* [43], qui concerne les carquois finis quelconques et la classification des indécomposables à isomorphisme près liée à la forme de Tits q. Pour un carquois fini, on sait encore définir des racines, mais cette fois, elles se partitionnent en racines *réelles* caractérisées par l'égalité $q(\mathbf{d}) = 1$, et racines *imaginaires* telles que $q(\mathbf{d}) \leqslant 0$. Les racines réelles sont en bijection avec les classes d'indécomposables qui correspondent à des orbites denses. En revanche, le problème des racines imaginaires est plus retors. Une racine imaginaire $\mathbf{d}$ correspond à une famille de classes d'indécomposables à plus de $1 - q(\mathbf{d})/2$ paramètres.

Le cas particulier où la forme de Tits est positive non définie est plus digeste. Les racines imaginaires correspondent à des familles de classes d'indécomposables paramétrées par $\mathbb{P}^1(\mathbb{C})$. C'est exactement ce que l'on peut voir illustré dans le *théorème de Jordan-Kronecker*, dont le carquois est $\bullet \rightleftarrows \bullet$ et la forme de Tits est donnée par $(x-y)^2$. Dans ce cas, les racines réelles sont $(n+1, n)$, $(n, n+1)$ $(n \in \mathbb{N})$ —les solutions dans $\mathbb{N}^2$ de $(x-y)^2 = 1$— et les racines imaginaires sont (n, n) —les solutions de $(x-y)^2 = 0$. Un simple regard sur l'énoncé du théorème de Jordan-Kronecker permet de mettre en lumière le théorème de Kac.

Encore un spécimen du type : la construction de l'invariant *birapport* à l'aide du carquois $\tilde{D}_4$ de l'exemple 8.7.

8. Retour au problème des N sous-espaces... et au-delà

Il serait temps de clore le chapitre. Toutefois, il serait préjudiciable de conclure sans avoir établi des liens solides entre la théorie des carquois et le problème de la classification de configurations de sous-espaces d'où nous étions partis en début de chapitre.

8.1. Problème des N sous-espaces, deuxième !

On fixe donc un espace E de dimension n et une base de E, nous permettant d'identifier E à $\mathbb{K}^n$. On veut, dans un premier temps, comprendre la classification de N sous-espaces $(F_1, \ldots, F_N)$ en termes de représentations de carquois.

On considère le carquois Q^N avec $N+1$ sommets $Q_0^N = \{0, 1, \dots, N\}$ et N flèches données par $Q_1^N = \{\alpha_1, \dots, \alpha_N\}$ telles que $s(\alpha_k) = k$, $t(\alpha_k) = 0$ si $1 \leqslant k \leqslant N$. Toute l'idée est de remplacer les inclusions $F_i \subset E$ par une flèche injective représentant l'inclusion de F_k dans $F_0 = E$.

On fixe $\mathbf{d} = (d_0, d_1, \dots, d_N) \in \mathbb{N}^{Q_0}$, avec $d_0 = n$ et $d_k \leqslant d_0$ si $1 \leqslant k \leqslant N$. On note $\mathscr{C}_{\mathbf{d}+}$, avec $\mathbf{d}^+ = (d_1, \dots, d_N)$, l'ensemble des configurations $(E; F_1, \dots, F_N)$ de sous-espaces telles que $\dim F_k = d_k$ pour tout k. Le groupe $\mathrm{GL}_n(\mathbb{K})$ agit sur $\mathscr{C}_{\mathbf{d}+}$ par $g\cdot(E; F_1, \dots, F_N) = \big(E; g(F_1), \dots, g(F_N)\big)$ et l'objet d'étude est l'ensemble quotient $\mathscr{C}_{\mathbf{d}+}/\mathrm{GL}_n(\mathbb{K})$ des configurations à isomorphisme près.

Par définition, on a : $\mathrm{Rep}_{\mathbf{d}} = \mathrm{Hom}(\mathbb{K}^{d_1}, \mathbb{K}^n) \oplus \cdots \oplus \mathrm{Hom}(\mathbb{K}^{d_N}, \mathbb{K}^n)$. On note $\mathrm{Rep}^0(Q^N) = \mathrm{Rep}^0$ l'ensemble des représentations V du carquois Q^N telles que chaque V_{α_k} soit injective et $\mathrm{Rep}^0_{\mathbf{d}} = \mathrm{Rep}^0 \cap \mathrm{Rep}_{\mathbf{d}}$. Il est clair que $\mathrm{Rep}^0_{\mathbf{d}}$ est stable pour l'action du groupe $G_{\mathbf{d}}$ sur $\mathrm{Rep}_{\mathbf{d}}$.

8.2. Exercice. *Montrer que si* $\mathbb{K}$ *est* $\mathbb{R}$ *ou* $\mathbb{C}$, *alors* $\mathrm{Rep}^0_{\mathbf{d}}$ *est un ouvert pour la topologie normique de* $\mathrm{Rep}_{\mathbf{d}}$.

On pourra appliquer la propriété de semi-continuité du rang, voir [H2G2, remarque I-4.4].

Étant donnée une représentation V du carquois Q^N, on lui associe la configuration $\Gamma_{\mathbf{d}}(V) = (E; \mathrm{im}\, V_{\alpha_1}, \dots, \mathrm{im}\, V_{\alpha_N})$.

8.3. Lemme. *Soit* $\mathbf{d} = (d_0, d_1, \dots, d_N) \in \mathbb{N}^{Q_0}$. *Avec les notations précédentes, l'application* Γ *définit une bijection* $\overline{\Gamma}$ *entre les classes d'isomorphisme* $\mathrm{Rep}^0_{\mathbf{d}}/G_{\mathbf{d}}$ *et l'ensemble des configurations à isomorphisme près* $\mathscr{C}_{\mathbf{d}+}/\mathrm{GL}_n(\mathbb{K})$.

Démonstration. Toute la preuve repose sur [H2G2, théorème IV-2.5] : l'application $\varphi \mapsto \mathrm{im}\,\varphi$ définit une surjection de l'ensemble des applications linéaires de rang r de F dans E vers la grassmannienne des sous-espaces vectoriels de E de dimension r. De plus, l'antécédent d'un sous-espace de dimension r est une seule orbite pour l'action à droite de $\mathrm{GL}(F)$ sur $\mathrm{Hom}_{\mathbb{K}}(F, E)$.

On vérifie que l'on définit bien une application Γ de $\mathrm{Rep}^0_{\mathbf{d}}$ sur $\mathscr{C}_{\mathbf{d}+}$. En notant que $G_{\mathbf{d}} = \mathrm{GL}_n(\mathbb{K}) \times G_{\mathbf{d}+}$, on obtient, par l'assertion qui précède, que l'action du sous-groupe $\{e\} \times G_{\mathbf{d}+}$ de $G_{\mathbf{d}}$ est invariante par Γ. On obtient aussi par la même assertion que l'antécédent d'une configuration de $\mathscr{C}_{\mathbf{d}+}$ est une seule orbite de $\mathrm{Rep}^0_{\mathbf{d}}$ pour l'action de $\{e\} \times G_{\mathbf{d}+}$.

Maintenant, Γ commute avec l'action de $\mathrm{GL}_n(\mathbb{K})$. Il en découle une application $\overline{\Gamma}$ bien définie de $\mathrm{Rep}^0_{\mathbf{d}}/G_{\mathbf{d}}$ vers $\mathscr{C}_{\mathbf{d}+}/\mathrm{GL}_n(\mathbb{K})$ et bijective d'après ce qui précède. □

Toute la théorie des représentations de carquois est fondée sur la décomposition en indécomposables et la classification des indécomposables à isomorphisme près. À présent, il reste donc à comprendre la décomposition de $\mathrm{Rep}^0_{\mathbf{d}}$ en indécomposables. C'est le but du lemme suivant.

8.4. Lemme. *Soit Q un carquois et soit $\mathbf{d} \in \mathbb{N}^{Q_0}$.*

(i) *Soient V une représentation de $\mathrm{Rep}^0_{\mathbf{d}}$ et $V' \in \mathrm{Rep}_{\mathbf{d}'}$ un facteur direct de V, alors on a : $V' \in \mathrm{Rep}^0_{\mathbf{d}'}$.*

(ii) *Une représentation ne peut pas se décomposer comme somme directe de représentations de $\bigcup_{\mathbf{d}'} \mathrm{Rep}^0_{\mathbf{d}'}$ si et seulement si elle ne peut pas se décomposer comme somme de représentations de $\bigcup_{\mathbf{d}'} \mathrm{Rep}_{\mathbf{d}'}$.*

(iii) *Inversement, soient $\mathbf{d}'$ et $\mathbf{d}''$ deux éléments de $\mathbb{N}^{Q_0}$ et soient $V' \in \mathrm{Rep}^0_{\mathbf{d}'}$ et $V'' \in \mathrm{Rep}^0_{\mathbf{d}''}$. On a alors : $V' \oplus V'' \in \mathrm{Rep}^0_{\mathbf{d}'+\mathbf{d}''}$.*

(iv) *L'application $\overline{\Gamma}$ commute avec les sommes directes.*

(v) *L'application $\overline{\Gamma}$ envoie des classes de représentations indécomposables sur des classes de configurations indécomposables.*

Démonstration. Pour les deux premiers points, il suffit d'appliquer pour chaque flèche du carquois Q le résultat suivant : pour $\varphi' \in \mathrm{Hom}_{\mathbb{K}}(M', N')$ et $\varphi'' \in \mathrm{Hom}_{\mathbb{K}}(M'', N'')$, alors $\varphi' \oplus \varphi''$ (qui appartient à $\mathrm{Hom}_{\mathbb{K}}(M' \oplus M'', N' \oplus N'')$) est injective si et seulement si φ' et φ'' le sont. Les autres découlent des définitions ou de ces deux premiers points. □

8.5. Exemple. Soit Q le carquois $1 \longrightarrow 0 \longleftarrow 2$, qui correspond aux configurations de deux sous-espaces F_1 et F_2 dans un espace $F_0 = E$. Les indécomposables de Rep^0 sont, d'après le théorème de Gabriel 7.7 et le lemme 8.4, les indécomposables I_0, I_1, I_2, I_{12} suivants caractérisés par leur vecteur de dimension :

$$\mathbf{dim}\, I_0 = (0,1,0),\ \mathbf{dim}\, I_1 = (1,1,0),\ \mathbf{dim}\, I_2 = (0,1,1),\ \mathbf{dim}\, I_{12} = (1,1,1).$$

À un couple de sous-espaces (F_1, F_2) correspond une représentation V de Q, qui possède une unique décomposition :

$$V = n_0 I_0 \oplus n_1 I_1 \oplus n_2 I_2 \oplus n_{12} I_{12} \quad (n_0, n_1, n_2, n_{12} \in \mathbb{N}).$$

Le lien entre la décomposition de V en indécomposables et les dimensions des sommes et intersections des F_i est donné par :

$$n_{12} = \dim(F_1 \cap F_2),\ n_i = \dim F_i - \dim(F_1 \cap F_2),\ n_0 = \dim E - \dim(F_1 + F_2).$$

Pour le montrer, il suffit, en vertu du lemme 8.4, de le faire pour les configurations/représentations indécomposables et d'utiliser l'additivité des membres de gauche et de droite vis-à-vis des sommes directes.

8.6. Exemple. Pour trois sous-espaces F_i dans un espace F_0, on prend :

$$\begin{array}{ccccc} & & 3 & & \\ & & \downarrow & & \\ 1 & \longrightarrow & 0 & \longleftarrow & 2. \end{array}$$

Les indécomposables de Rep^0 sont, d'après le théorème de Gabriel 7.7 et le lemme 8.4, les indécomposables suivants : I_0, où l'espace $\mathbb{K}$ est concentré au sommet 0 ; I_i $(1 \leqslant i \leqslant 3)$, où l'espace $\mathbb{K}$ est concentré au sommet i et au sommet 0 ; I_{ij} $(1 \leqslant i < j \leqslant 3)$, où l'espace $\mathbb{K}$ est concentré aux sommets i, j et 0 ; I_{123} où l'espace $\mathbb{K}$ est placé sur tous les sommets ; enfin I'_{123}, où l'espace $\mathbb{K}$ est placé sur les sommets $i \neq 0$ et où $\mathbb{K}^2$ est placé au sommet 0.

À un triplet de sous-espaces (F_1, F_2, F_3) correspond la représentation :

$$V = \bigoplus_{i=0}^{3} n_i I_i \oplus \bigoplus_{1 \leqslant i < j \leqslant 3} I_{ij} \oplus n_{123} I_{123} \oplus n'_{123} I'_{123}.$$

Le lien entre la décomposition de V en indécomposables et les dimensions des sommes et intersections des F_i est donné par

$$\begin{aligned} n_0 &= \dim F_0 - \dim(F_1 + F_2 + F_3), \\ n_i &= \dim(F_1 + F_2 + F_3) + \dim F_j \cap F_k - \dim F_j - \dim F_k \quad (0, i, j, k \text{ distincts}), \\ n_{ij} &= \dim F_i \cap F_j - \dim F_1 \cap F_2 \cap F_3 \quad (i < j), \\ n_{123} &= \dim F_1 \cap F_2 \cap F_3, \\ n'_{123} &= -\dim(F_1 + F_2 + F_3) + \sum_{i=1}^{3} \dim F_i - \sum_{i<j} \dim F_i \cap F_j + \dim F_1 \cap F_2 \cap F_3. \end{aligned}$$

La preuve est la même que dans l'exemple précédent.

8.7. Exemple. Soit Q le carquois des quatre sous-espaces « de type $\tilde{D}_4$ » :

$$\begin{array}{ccccc} & & 3 & & \\ & & \downarrow & & \\ 1 & \longrightarrow & 0 & \longleftarrow & 2 \\ & & \uparrow & & \\ & & 4 & & \end{array}$$

Il y a une belle histoire sur le carquois Q. On considère le vecteur de dimension $\mathbf{d} = (2, 1, 1, 1, 1)$. L'étude de $\mathscr{C}_{\mathbf{d}} / \mathrm{GL}_2(\mathbb{K})$ peut être abordée de deux façons différentes :

- soit par [H2G2, proposition X-1.2.16], car on sait que l'ensemble de quatre droites en configuration dans le plan, modulo $\mathrm{GL}_2(\mathbb{K})$, est paramétré par le birapport (dans $\mathbb{P}^1$) ; en particulier, sur un corps infini, il y a une infinité d'orbites ;

– soit par la correspondance entre $\mathrm{Rep}^0_{\mathbf{d}}/G_{\mathbf{d}}$ et $\mathscr{C}_{\mathbf{d}}/\mathrm{GL}_2(\mathbb{K})$; en notant q la forme de Tits, on a : $q(2,1,1,1,1) = 2^2 + 4 \times 1 - 4 \times 2 \times 1 = 0$ et le théorème de Kac (admis) assure qu'il existe une famille de représentations indécomposables V_λ ; par indécomposabilité, elles sont nécessairement dans Rep^0 (admis) ; si $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$, $[V_\lambda, V_\lambda] \geqslant 1 - q(\mathbf{d}) = 1$ et donc, par la proposition 6.8, il y a une infinité d'orbites.

Il en résulte, pour le carquois Q^N avec $N \geqslant 4$, que si $d_0 \geqslant 2$, et $d_i \geqslant 1$ pour au moins quatre valeurs de i, alors $\mathscr{C}_{\mathbf{d}}/\mathrm{GL}_2(\mathbb{K})$ ne peut posséder un nombre fini d'indécomposables. En effet, quitte à choisir $d_i \geqslant 1$ pour $1 \leqslant i \leqslant 4$, on peut écrire $\mathbf{d} = (2,1,1,1,1,0,\ldots,0) + \mathbf{d}'$ et en fixant une représentation V' de $\mathrm{Rep}^0_{\mathbf{d}'}$, on a une infinité de représentations de la forme $V_\lambda \oplus V'$ et ces représentations sont non isomorphes par le théorème de Krull-Schmidt.

8.8. Problème des N drapeaux

On aurait tort de croire que la problématique s'arrête là : reformulons en termes de grassmanniennes les résultats obtenus. On considère l'action du groupe $\mathrm{GL}_n(\mathbb{C})$ sur le produit de grassmanniennes $\mathrm{Gr}_{m_1,n} \times \cdots \times \mathrm{Gr}_{m_k,n}$, donnée par l'action diagonale $g \cdot (F_1, \ldots, F_k) = \big(g(F_1), \ldots, g(F_k)\big)$. Évitons les cas triviaux en supposant $n \geqslant 2$ et $m_i \geqslant 1$ si $1 \leqslant i \leqslant k$. Alors, cette action possède un nombre fini d'orbites si et seulement si $k \leqslant 3$. Ce problème se généralise sans difficulté à celui de l'étude de l'action de $\mathrm{GL}_n(\mathbb{C})$ sur le produit de variétés de drapeaux.

On va définir la *variété des drapeaux associée à une composition*, objet intermédiaire entre la grassmannienne et la variété des drapeaux complets.

8.9. Définition. Soit $n \in \mathbb{N}$. Une *composition* $\mathbf{a} = (a_1, \ldots, a_k)$ de n désigne une k-liste d'entiers naturels dont la somme est égale à n. On note $\mathscr{FL}_{\mathbf{a}}$ l'ensemble des $(k+1)$-listes $(F_0, F_1, \ldots, F_k)$ de sous-espaces de $\mathbb{K}^n$ tels que $0 = F_0 \subset F_1 \subset \cdots \subset F_k$ et $\dim F_j - \dim F_{j-1} = a_j$ pour tout j entre 1 et k.

Le groupe $\mathrm{GL}_n(\mathbb{K})$ agit naturellement sur $\mathscr{FL}_{\mathbf{a}}$ vu comme sous-ensemble de produits de grassmanniennes. Une N-liste $(\mathbf{a}_1, \ldots, \mathbf{a}_N)$ de compositions de n est dite *de type fini* si le nombre d'orbites de $\mathrm{GL}_n(\mathbb{K})$ pour l'action diagonale sur $\mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N}$ est fini.

La grassmannienne $\mathrm{Gr}_{m,n}$ s'identifie à $\mathscr{FL}_{(m,n-m)}$ et l'on voit bien que le problème de la classification des N-listes de compositions de n de type fini généralise l'étude faite ci-dessus sur les grassmanniennes.

On fixe N compositions de n, $\mathbf{a}_i = (a_{ij})$ $(1 \leqslant i \leqslant N,\ 1 \leqslant j \leqslant k_i)$ et on considère le carquois étoilé Q à N branches de la figure 8.1, qui suit.

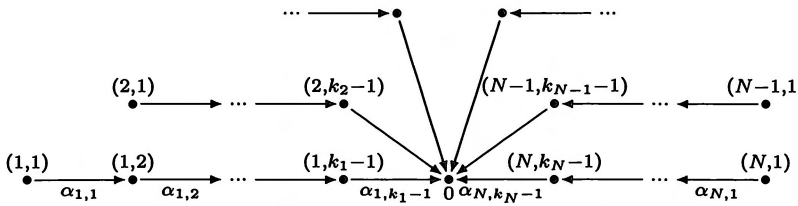


Figure 8.1. *Carquois étoilé à N branches*

Formellement : $Q_0 = \{0\} \cup \big\{(i,j) : 1 \leqslant i \leqslant N,\ 1 \leqslant j \leqslant k_i - 1\big\}$, $Q_1 = \{\alpha_{ij} : 1 \leqslant i \leqslant N,\ 1 \leqslant j \leqslant k_i - 1\}$, où α_{ij} est la flèche $(i,j) \to (i,j+1)$ si $1 \leqslant j \leqslant k_i - 2$ et $\alpha_{i(k_i-1)}$ est $(i,k_i-1) \to 0$.

Pour utiliser le théorème de Gabriel, on travaille sur le corps $\mathbb{C}$.

8.10. Proposition. *Soit n un entier naturel, soit $\mathbf{a}_i = (a_{ij})$ $(1 \leqslant i \leqslant N,\ 1 \leqslant j \leqslant k_i)$ une N-liste de compositions de n et soit Q le carquois associé. Soit $\mathbf{d} \in \mathbb{N}^{Q_0}$ tel que $d_0 = n$, $d_{(i,j)} = a_{i1} + \cdots + a_{ij}$. Soient $G_{\mathbf{d}} = \prod_{s \in Q_0} \mathrm{GL}_{d_s}$ et $G_{\mathbf{d}+} = \prod_{s \in Q_0, s \neq 0} \mathrm{GL}_{d_s}$.*

Alors, il existe un bijection naturelle $\mathrm{Rep}^0_{\mathbf{d}}(Q)/G_{\mathbf{d}+} \simeq \mathscr{F}\mathscr{L}_{\mathbf{a}_1} \times \cdots \times \mathscr{F}\mathscr{L}_{\mathbf{a}_N}$ qui, après passage au quotient, établit une bijection :

$$\mathrm{Rep}^0_{\mathbf{d}}(Q)/G_{\mathbf{d}} \simeq (\mathscr{F}\mathscr{L}_{\mathbf{a}_1} \times \cdots \times \mathscr{F}\mathscr{L}_{\mathbf{a}_N})/\,\mathrm{GL}_n(\mathbb{K}).$$

Démonstration. À une représentation à flèches injectives V de Q, de vecteur de dimension $\mathbf{d}$, et pour tout i de 1 à N, on associe le drapeau $\mathscr{F}\mathscr{L}(V)$:

$$0 \subset \mathrm{im}\big(V_{i(k_i-1)} \cdots V_{i1}\big) \subset \mathrm{im}\big(V_{i(k_i-1)} \cdots V_{i2}\big) \subset \cdots \subset \mathrm{im}\, V_{i(k_i-1)} \subset \mathbb{K}^n,$$

où l'on a noté V_{ij} pour $V_{\alpha_{ij}}$ au nom de l'esthétique et du bon goût.

On vérifie qu'il s'agit bien, par construction du carquois et par injectivité des flèches, d'un drapeau de $\mathscr{F}\mathscr{L}_{\mathbf{a}_i}$. Et donc, on a construit une application de $\mathrm{Rep}^0_{\mathbf{d}}(Q)$ vers $\mathscr{F}\mathscr{L}_{\mathbf{a}_1} \times \cdots \times \mathscr{F}\mathscr{L}_{\mathbf{a}_N}$. Cette application passe au quotient pour l'action de $G_{\mathbf{d}+}$.

On laisse le soin au lecteur consciencieux de montrer qu'il s'agit bien d'une bijection ainsi que la dernière assertion à l'aide du lemme 8.3. □

8.11. Remarque. Voir l'exercice E.11 pour une bijection explicite dans un cas particulier.

8.12. Corollaire. *Soit $\mathbf{a} = (\mathbf{a}_1, \ldots, \mathbf{a}_m)$ une N-liste de compositions de n. Si le carquois Q associé est de type A, D ou E, alors $\mathbf{a}$ est de type fini.*

8.13. Exemple. L'action de $\mathrm{GL}_5(\mathbb{C})$ sur $\mathscr{FL}_{(1,1,1,1,1)} \times \mathscr{FL}_{(2,1,2)} \times \mathrm{Gr}_{2,5}$ possède un nombre fini d'orbites, dont il suffirait d'un peu de patience pour en calculer le nombre. En effet, pour $\mathbf{a} = \big((1,1,1,1,1),(2,1,2),(2,3)\big)$ le carquois associé à $\mathbf{a}$ est de type E_8.

8.14. Exemple (Ringel). La réciproque du corollaire est fausse, quoique les contre-exemples soient en séries limitées d'après [49]. On peut, en admettant le théorème de Kac, en comprendre la raison via ce contre-exemple dû à Ringel. On fait agir $\mathrm{GL}_4(\mathbb{C})$ sur $\mathscr{FL}_{(1,1,1,1)} \times \mathscr{FL}_{(1,1,1,1)} \times \mathscr{FL}_{3,1}$. Le carquois associé est un carquois de type $\tilde{E}_7$ (définition B.4). Ce n'est donc pas un carquois de type fini A, D, E. Par la bijection établie dans la proposition, on étudie les orbites dans l'espace de représentations $\mathrm{Rep}^0_{\mathbf{d}}$, où $\mathbf{d} = (4,1,2,3,1,2,3,3)$. Soit q la forme de Tits associée au carquois, on trouve : $q(\mathbf{d}) = 1$. Mais, si l'on pose $\mathbf{d}' = (4,1,2,3,1,2,3,2)$, on obtient $q(\mathbf{d}') = 0$ et $\mathbf{d} = \mathbf{d}' + \mathbf{d}''$, avec $\mathbf{d}'' = (0,0,0,0,0,0,0,1)$. Il y a donc, par le théorème de Kac, une infinité de classes d'indécomposables I_λ de vecteur de dimension $\mathbf{d}'$, et joint à une représentation simple S de vecteur de dimension $\mathbf{d}''$, on trouve une infinité de classes $I_\lambda \oplus S$ de vecteur de dimension $\mathbf{d}$. Comme $\tilde{E}_7$ est de type affine (définition B.4), sa forme de Tits est positive non définie (théorème B.6) et on peut voir que celle-ci possède une unique droite isotrope de direction $\mathbf{d}'$. On vérifie alors qu'une écriture $\mathbf{d} = \mathbf{d}_1 + \mathbf{d}_2$ (pour des vecteurs entiers positifs) avec $q(\mathbf{d}_1) = 0$ n'est possible que si $\mathbf{d}_1 = \mathbf{d}'$ et $\mathbf{d}_2 = \mathbf{d}''$. Or, une représentation de $\mathrm{Rep}^0(Q)$ ne peut pas posséder dans sa décomposition une représentation indécomposable de vecteur de dimension $\mathbf{d}''$. On déduit de tout cela qu'il ne peut exister qu'un nombre fini de représentations injectives à isomorphisme près de vecteur de dimension $\mathbf{d}$. Ainsi, l'ensemble $\big(\mathscr{FL}_{(1,1,1,1)} \times \mathscr{FL}_{(1,1,1,1)} \times \mathscr{FL}_{3,1}\big)/\mathrm{GL}_4(\mathbb{C})$ est fini.

Il est tentant de se demander si les bijections de la proposition 8.10 sont des homéomorphismes. Si c'est le cas, on a un transport de structure dans les ordres de dégénérescence. On note encore $\leqslant_{\mathrm{deg}}$ la relation de (pré)ordre de dégénérescence des orbites de $\mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N}$ pour l'action de $\mathrm{GL}_n(\mathbb{K})$, définie ainsi : $w \leqslant_{\mathrm{deg}} w'$ dans $\mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N} / \mathrm{GL}_n(\mathbb{K})$ si $\mathscr{O}_w \leqslant \mathscr{O}_{w'}$ dans $\mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N}$. Pour une représentation V dans $\mathrm{Rep}^0_{\mathbf{d}}$, on note $w_V \in \mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N} / \mathrm{GL}_n(\mathbb{K})$ l'orbite qui lui correspond.

8.15. Corollaire. *L'application qui à V dans $\mathrm{Rep}^0_{\mathbf{d}}$ associe la classe de w_V dans $\mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N} / \mathrm{GL}_n(\mathbb{K})$ est continue et les bijections de la proposition 8.10 sont des homéomorphismes.*

On a de plus : $V \leqslant_{\mathrm{deg}} V'$ si et seulement si $w_V \leqslant_{\mathrm{deg}} w_{V'}$. En particulier, la relation $\leqslant_{\mathrm{deg}}$ est bien un ordre sur $\mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N} / \mathrm{GL}_n(\mathbb{K})$.

Démonstration. La continuité de $V \mapsto \mathscr{FL}(V) = w_V$ est une conséquence directe de la continuité de l'application im sur l'ouvert des matrices de rang maximum, voir l'exercice I-C.4. De plus, comme l'application im définit un homéomorphisme $\mathscr{M}^0_{n,m}/\operatorname{GL}_m(\mathbb{K}) \simeq \operatorname{Gr}_{m,n}$, on obtient par récurrence sur le nombre de flèches du carquois Q un homéomorphisme

$$\Phi : \operatorname{Rep}^0_{\mathbf{d}}(Q)/G_{\mathbf{d}+} \xrightarrow{\sim} \mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N},$$

puis un homéomorphisme $\operatorname{Rep}^0_{\mathbf{d}}(Q)/G_{\mathbf{d}} \simeq \mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N} / \operatorname{GL}_n(\mathbb{K})$ après passage au quotient.

La continuité de $V \mapsto \mathscr{FL}(V) = w_V$ donne : $V \leqslant_{\deg} V' \Rightarrow w_V \leqslant_{\deg} w_{V'}$.

Pour la réciproque, on montre que si l'on a : $\mathscr{O}_{w_V} \subset \overline{\mathscr{O}_{w_{V'}}}$ dans $\mathscr{FL}_{\mathbf{a}_1} \times \cdots \times \mathscr{FL}_{\mathbf{a}_N}$, alors on a aussi : $\mathscr{O}_V \subset \overline{\mathscr{O}_{V'}}$ dans $\operatorname{Rep}^0_{\mathbf{d}}$. Grâce à l'homéomorphisme Φ ci-dessus, il suffit de montrer, avec $X = \operatorname{Rep}^0_{\mathbf{d}}$, $G = G_{\mathbf{d}+}$ et π la projection $X \to Y = X/G$, que pour toute partie B de Y, on a : $\overline{\pi^{-1}(B)} = \pi^{-1}(\overline{B})$.

Montrons cette assertion. L'inclusion est claire car π est continue. Maintenant, $\overline{\pi^{-1}(B)}$ et $\pi^{-1}(\overline{B})$ sont des réunions d'orbites, pour $\pi^{-1}(\overline{B})$, c'est clair, pour $\overline{\pi^{-1}(B)}$, ça l'est aussi par continuité de l'action de G sur X. Afin de montrer l'inclusion, il suffit de montrer $\pi\big(\pi^{-1}(\overline{B})\big) \subset \pi\big(\overline{\pi^{-1}(B)}\big)$. Or, comme π est surjective et ouverte, $\pi\big(\overline{\pi^{-1}(B)}\big) = \overline{\pi\big(\pi^{-1}(B)\big)} = \overline{B}$ et l'inclusion en résulte.

Pour finir, on sait par la proposition 6.11 que la relation $\leqslant_{\deg}$ est un ordre sur $\operatorname{Rep}_{\mathbf{d}}$; cette propriété entraîne avec elle la dernière assertion. □

If you want to be a hero, well just follow me.
John Lennon, *Working Class Hero*, 1970.

A. Annexe. Algèbre de chemins et théorie des représentations

On fixe dans toute l'annexe un carquois Q fini et un corps $\mathbb{K}$.

Après les avoir considérées comme des collections d'espaces (V_i) et d'applications linéaires (V_α), puis comme des points dans un « espace de représentation » $\mathrm{Rep}_{\mathbf{d}}$, nous allons poser un troisième regard sur les représentations du carquois Q et les voir comme modules sur une algèbre (non commutative) adaptée au contexte. Cette vision permet d'utiliser des théorèmes classiques pour montrer l'unicité de la décomposition (*théorème de Krull-Schmidt*), l'utilisation des noyaux, des suites exactes, des extensions... Pour donner une idée de la chose, on va généraliser la pratique qui consiste à remplacer l'étude des endomorphismes d'un $\mathbb{K}$-espace vectoriel par celle de $\mathbb{K}[X]$-modules, voir II-A. Nous verrons alors une troisième interprétation des invariants $[V,W]^0$ et $[V,W]^1$.

A.1. Définition. On appelle *chemin* du carquois Q une suite finie de la forme $c=(y,\alpha_n,\alpha_{n-1},\dots,\alpha_1,x)$, où $x,y\in Q_0$, $n\in\mathbb{N}$, $\alpha_i\in Q_1$, $s(\alpha_1)=x$, $t(\alpha_i)=s(\alpha_{i+1})$ si $1\leqslant i<n$, $t(\alpha_n)=y$. On pose alors $s(c)=x$ (la *source* du chemin c est x), $t(c)=y$ (le *terminus* du chemin c est y) et $\ell(c)=n$ (la *longueur* du chemin c est n).

Le *chemin paresseux* associé au sommet i est le chemin $e_i=(i,i)$. Il est de longueur 0.

Deux chemins c et c' sont dits *composables* si $s(c)=t(c')$. Le *produit* ou la *composée* $c\cdot c'$ des chemins est alors défini par concaténation :

$$c\cdot c'=(y,\alpha_n,\alpha_{n-1},\dots,\alpha_1,\alpha'_{n'},\dots,\alpha'_1,x')$$

où $c=(y,\alpha_n,\alpha_{n-1},\dots,\alpha_1,x)$ et $c'=(x,\alpha'_{n'},\alpha'_{n'-1},\dots,\alpha'_1,x')$.

On notera $\mathscr{C}_Q$ —ou simplement $\mathscr{C}$ si aucune confusion n'est à craindre— l'ensemble des chemins du carquois Q.

A.2. Définition. Soit $\mathbb{K}Q=\mathbb{K}^{\mathscr{C}_Q}$ l'espace des combinaisons linéaires formelles de chemins de $\mathscr{C}_Q$: c'est un espace vectoriel sur $\mathbb{K}$ dont $\mathscr{C}_Q$ est une base. Pour deux chemins c et c' de $\mathscr{C}_Q$, on pose :

$$cc'=\begin{cases} c\cdot c' & \text{si } c \text{ et } c' \text{ sont composables}\\ 0 & \text{sinon.}\end{cases}$$

On prolonge cette application en une application bilinéaire $\mathbb{K}Q\times\mathbb{K}Q\to\mathbb{K}Q$. On définit ainsi une structure d'algèbre sur $\mathbb{K}Q$ appelée *algèbre des chemins* de Q (sur $\mathbb{K}$).

A.3. Remarque. L'algèbre $\mathbb{K}Q$ est associative et admet une unité (on rappelle que Q_0 est fini) : $1 = \sum_{i \in Q_0} e_i$. Les chemins paresseux e_i ($i \in Q_0$) sont des *idempotents* orthogonaux de l'algèbre des chemins, c'est-à-dire que l'on a : $e_i^2 = e_i$ pour tout i et $e_i e_j = 0$ si $i \neq j$.

A.4. Exemple. Si le carquois Q est réduit à un sommet sans flèche, soit $\bullet$, alors $\mathbb{K}Q = \mathbb{K}$. Si Q est un carquois sans flèches (autrement dit, $Q_1 = \emptyset$), alors on a : $\mathbb{K}Q = \bigoplus_{i \in Q_0} \mathbb{K}e_i$; c'est un produit direct de corps.

A.5. Exemple. Si Q est la boucle ($|Q_0| = 1$, $|Q_1| = 1$), on a : $\mathbb{K}Q \simeq \mathbb{K}[X]$. Si Q est une double boucle ($|Q_0| = 1$, $|Q_1| = 2$), $\mathbb{K}Q$ est l'algèbre non commutative libre $\mathbb{K}\langle X, Y\rangle$ à deux générateurs.

A.6. Exemple. Pour le carquois Q : $1 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3$, l'algèbre $\mathbb{K}Q$ est isomorphe à l'algèbre des matrices 3×3 triangulaires inférieures. Plus précisément, avec les notations standard des matrices élémentaires, l'isomorphisme est défini par $e_i \mapsto E_{ii}$, $\alpha \mapsto E_{21}$, $\beta \mapsto E_{32}$, $\beta \cdot \alpha \mapsto E_{31}$.

A.7. Représentations de Q et modules sur $\mathbb{K}Q$

Le but de ce paragraphe est de décrire une correspondance entre représentations de carquois et $\mathbb{K}Q$-modules (de dimension finie).

Représentations de carquois $\rightsquigarrow$ $\mathbb{K}Q$-modules. Soit V une représentation du carquois Q. On définit le $\mathbb{K}Q$-module $F(V)$ ainsi :

- comme $\mathbb{K}$ espace : $F(V) = \bigoplus_{i \in Q_0} V_i$;
- comme $\mathbb{K}Q$ module :
  - ▷ pour $i \in Q_0$, le chemin paresseux e_i agit sur $F(V)$ comme la projection sur V_i compatible avec la décomposition ci-dessus de $F(V)$;
  - ▷ si $c = (j, \alpha_n, \ldots, \alpha_1, i)$ et $m \in F(V)$, alors

$$c \cdot m = \iota_j \circ V_{\alpha_n} \circ \cdots \circ V_{\alpha_1} \circ \pi_i(m),$$

où $\iota_j : V_j \to V$ est l'injection naturelle (un peu là pour faire joli et rendre la chose symétrique !).

Soit $\phi = (\phi_i)_{i \in Q_0}$ un morphisme de représentations entre V et W. On définit naturellement un morphisme de $\mathbb{K}Q$-modules de $F(V)$ vers $F(W)$ par $F(\phi) = \bigoplus_i \phi_i$ (la somme par blocs des applications linéaires de V_i vers W_i).

On vérifie en exercice que l'on a bien défini une structure de $\mathbb{K}Q$-modules sur $F(V)$, c'est-à-dire un morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}Q$ vers $\mathrm{End}\big(F(V)\big)$. La seule petite difficulté est de montrer que $c \cdot (c' \cdot m) = (cc') \cdot m$ pour tout c, c' de $\mathscr{C}_Q$ et tout m de $F(V)$, que l'on surmonte en se ramenant

au cas où c, c' sont les générateurs naturels de $\mathbb{K}Q$. On vérifie également que $F(\phi)$ est bien un morphisme de $\mathbb{K}Q$-modules tel que $F(\mathrm{Id}_V) = \mathrm{Id}_{F(V)}$ et $F(\phi \circ \phi') = F(\phi) \circ F(\phi')$. Ces vérifications ne devraient pas poser de difficulté.

$\mathbb{K}Q$-modules $\rightsquigarrow$ représentations de carquois. Soit M un $\mathbb{K}Q$-module de dimension finie sur $\mathbb{K}$. On forme la représentation $G(M)$ du carquois Q ainsi :

- pour tout i de Q_0, l'espace $G(M)_i$ associé au sommet i est l'espace $e_i M$;
- pour tout α de Q_1, l'application linéaire $G(M)_\alpha$ associée à α est :

$$G(M)_\alpha : e_{s(\alpha)}M \longrightarrow e_{t(\alpha)}M, \quad m \longmapsto c_\alpha m,$$

où $c_\alpha = \big(t(\alpha), \alpha, s(\alpha)\big) \in \mathbb{K}Q$ est le chemin associé à α.

On vérifie que $G(M)_\alpha$ est bien défini, c'est-à-dire que son image est bien dans $e_{t(\alpha)}M$: cela provient du fait que $c_\alpha m = \big(e_{t(\alpha)}c_\alpha\big)m = e_{t(\alpha)}(c_\alpha m)$.

Soit ψ un morphisme de $\mathbb{K}Q$-modules entre M et N. On définit le morphisme de représentations $G(\psi)$ de $G(M)$ vers $G(N)$ par $G(\psi)_i(m) = \psi(m)$. Il faut vérifier qu'il envoie bien $e_i M$ sur $e_i N$ et que l'on obtient des diagrammes commutatifs comme dans la définition 4.3. Cela est assuré par le fait que ψ est un morphisme de $\mathbb{K}Q$-modules. On vérifie également que $G(\mathrm{Id}_M) = \mathrm{Id}_{G(M)}$ et $G(\psi \circ \psi') = G(\psi) \circ G(\psi')$.

De plus, $FG(M) = M$ comme $\mathbb{K}Q$-module, avec $FG(\phi) = \phi$ et $GF(V) = V$ comme représentation de Q avec $GF(\psi) = \psi$.

Conclusion. Il est équivalent de parler de représentations de Q et de $\mathbb{K}Q$-modules, de morphismes de représentations et de morphismes de $\mathbb{K}Q$-modules. Entre autres, on pourra identifier $\mathrm{Hom}_{\mathbb{K},Q}$ et $\mathrm{Hom}_{\mathbb{K}Q}$ et, par abus de notation, on écrira V pour $F(V)$ ou M pour $G(M)$.

A.8. Le lemme de Fitting et le théorème de Krull-Schmidt

Notons que les correspondances ci-dessus commutent avec la somme directe et mettent ainsi en relation Q-représentations indécomposables et $\mathbb{K}Q$-modules indécomposables.

On peut alors tirer un premier bénéfice de cette identification. En effet, l'unicité à isomorphisme près de la décomposition en indécomposables est une propriété générale connue sous le nom de théorème de Krull-Schmidt. Vu le contexte, nous le démontrerons dans le cadre des modules de dimension finie sur une $\mathbb{K}$-algèbre. Le lecteur pourra voir dans [46] la preuve dans un cadre plus général[19].

[19] L'hypothèse cruciale est la finitude des chaînes décroissantes d'idéaux ou de sous-modules (DCC en anglais pour *descending chain condition*), en contrepoint à l'hypothèse usuelle de noethérianité.

Avant d'attaquer, commençons par le *lemme de Fitting*, dont le nom cache l'importance. D'une part, il possède des applications dans des domaines divers ; d'autre part, il possède plusieurs avatars et corollaires puissants. En voici une version utile dans l'immédiat pour le cadre du théorème de Krull-Schmidt.

A.9. Proposition (lemme de Fitting, v. 1). *Soit E un espace vectoriel de dimension finie et soit u un endomorphisme de E. On note* $\ker u^\infty$ *(resp.* $\operatorname{im} u^\infty$*), la limite de la suite (stationnaire) des noyaux emboîtés (resp. des images emboîtées) de u. Alors :* $E = \ker u^\infty \oplus \operatorname{im} u^\infty$.

Démonstration. Par la formule du rang, on a : $\dim \ker u^\infty + \dim \operatorname{im} u^\infty = \dim E$. Il suffit donc de montrer que l'intersection des deux sous-espaces est triviale. Soit x dans l'intersection $\ker u^\infty \cap \operatorname{im} u^\infty = \ker u^n \cap \operatorname{im} u^n$, où on a choisi n assez grand. Alors, il existe un y tel que $x = u^n(y)$. On a donc : $0 = u^n(x) = u^{2n}(y)$. Il vient : $y \in \ker u^{2n} = \ker u^n$, ce qui implique : $x = u^n(y) = 0$. □

On peut voir cette version du lemme de Fitting à l'œuvre pour calculer le nombre d'endomorphismes nilpotents sur un corps fini, voir l'exercice IV-A.5.

A.10. Corollaire. *Soit E un espace vectoriel de dimension finie et soit u un endomorphisme de E. Alors, E se décompose en somme directe de deux sous-espaces F et G stables par u tels que u_F est nilpotent et u_G est un automorphisme de G.*

Démonstration. Il suffit de prendre : $F = \ker u^\infty$ et $G = \operatorname{im} u^\infty$. Bien sûr, l'endomorphisme u stabilise ces deux sous-espaces et induit un endomorphisme nilpotent sur le premier. De plus, on a : $\ker u \cap G \subset \ker u^\infty \cap G = \{0\}$, de sorte que u_G est bien un automorphisme de G. □

Le lemme de Fitting se traduit par une contrainte structurelle forte sur l'anneau des endomorphismes d'un A-module indécomposable de dimension finie.

A.11. Corollaire. *Soit A une $\mathbb{K}$-algèbre et soit M un A-module indécomposable de dimension finie sur $\mathbb{K}$. Alors, tout élément non inversible de* $\operatorname{End}_A(M)$ *est nilpotent. De plus, la somme de deux non inversibles de* $\operatorname{End}_A(M)$ *est encore non inversible.*

Démonstration. Soit u un élément non inversible de $\operatorname{End}_A(M)$. Son noyau n'est pas trivial et, *a fortiori*, $\ker u^\infty$ non plus. Par la proposition A.9, le A-module M se décompose en somme directe de $\ker u^\infty$ et $\operatorname{im} u^\infty$. Étant donné que M est indécomposable, on a : $\operatorname{im} u^\infty = \{0\}$, et donc u est nilpotent.

Soient u_1 et u_2 deux nilpotents de $\mathrm{End}_A(M)$ et $v = u_1 + u_2$. Supposons v inversible. Alors, les éléments $v_1 = v^{-1}u_1$ et $v_2 = v^{-1}u_2$ sont non inversibles et leur somme est : $v_1 + v_2 = \mathrm{Id}_M$. Cette dernière relation implique en particulier que v_1 et v_2 commutent, et comme par ce qui précède, v_1 et v_2 sont nilpotents, il vient que $v_1 + v_2 = \mathrm{Id}_M$ est nilpotent. Absurbe. □

En fait, cette propriété possède une réciproque. On dit qu'un anneau est *local* s'il possède un unique idéal maximal. Voici une version un peu améliorée du lemme de Fitting, appelée également... lemme de Fitting.

A.12. Corollaire. *Soit A une $\mathbb{K}$-algèbre, et soit M un A-module de dimension finie sur $\mathbb{K}$. Alors, M est indécomposable si et seulement si l'anneau $\mathrm{End}_A(M)$ est local.*

Démonstration. Supposons que M indécomposable. Alors l'ensemble $\mathfrak{m}$ des endomorphismes non inversibles est un idéal de $\mathrm{End}_A(M)$ par le corollaire A.11. Un idéal propre de $\mathrm{End}_A(M)$ ne contient aucun inversible, et il est donc inclus dans $\mathfrak{m}$: par suite, $\mathfrak{m}$ est l'unique idéal maximal.

Réciproquement, supposons que M soit décomposable, disons $M = M_1 \oplus M_2$ avec M_1 et M_2 non triviaux. Montrons que $\mathrm{End}_A(M)$ ne peut être local. Pour cela, il suffit de montrer que l'ensemble des éléments non inversibles n'est pas un idéal : en effet, dans un anneau local B, l'idéal maximal est constitué des éléments non inversibles, car tout élément non inversible non nul appartient à un idéal non trivial.

Soit π_1 (resp. π_2) la projection de M sur M_1 (resp. M_2). Alors, π_1 et π_2 sont deux éléments non inversibles de $\mathrm{End}_A(M)$, alors que $\pi_1 + \pi_2 = \mathrm{Id}_M$ est inversible. Donc l'ensemble des non inversibles ne constitue pas un groupe pour l'addition. □

Allez, zou ! Un cas particulier sur un corps algébriquement clos.

A.13. Corollaire. *Soit A une $\mathbb{K}$-algèbre sur un corps $\mathbb{K}$ algébriquement clos et soit M un A-module indécomposable de dimension finie. Alors, tout endomorphisme du A-module M est somme d'une homothétie et d'un endomorphisme nilpotent.*

Démonstration. Soit u dans $\mathrm{End}_A(M)$. Comme $\mathbb{K}$ est algébriquement clos, l'endomorphisme u possède une valeur propre λ dans $\mathbb{K}$. On applique la proposition A.9 à $u - \lambda\,\mathrm{Id}_M$ pour obtenir : $M = \ker(u - \lambda\,\mathrm{Id}_M)^\infty \oplus \mathrm{im}(u - \lambda\,\mathrm{Id}_M)^\infty$. Comme par hypothèse, $\{0\} \neq \ker(u - \lambda\,\mathrm{Id}_M) \subset \ker(u - \lambda\,\mathrm{Id}_M)^\infty$, il vient par indécomposabilité de M : $\ker(u - \lambda\,\mathrm{Id}_M)^\infty = M$. Donc, $u - \lambda\,\mathrm{Id}_M$ est nilpotent, ce qui prouve le corollaire. □

L'omniprésent *théorème de Krull-Schmidt* donne l'unicité de la décomposition en indécomposables.

A.14. Théorème (Krull-Schmidt). *Soit A une $\mathbb{K}$-algèbre et soit M un A-module de dimension finie sur $\mathbb{K}$. On considère deux décompositions de M en somme directe de A-modules indécomposables*

$$\bigoplus_{i=1}^{s} M_i = M = \bigoplus_{i'=1}^{s'} M'_{i'}.$$

Alors, $s = s'$ et il existe une permutation σ de $\mathfrak{S}_s$ telle que les A-modules M_i et $M'_{\sigma(i)}$ sont isomorphes pour tout i.

Démonstration. Commençons par trouver un entier $\sigma(1)$ dans $[1, s']$ de sorte que M_1 soit isomorphe à $M'_{\sigma(1)}$.

Pour tout i de $[1, s]$ (resp. $[1, s']$), on note π_i (resp. π'_i) la projection sur M_i (resp. M'_i) parallèlement à $\bigoplus_{j\neq i} M_j$ (resp. $\bigoplus_{j\neq i} M'_j$).

Pour i dans $[1, s']$, soient $\varpi_i : M'_i \to M_1$, $m \mapsto \pi_1(m)$ et $\varpi'_i : M_1 \to M'_i$, $m \mapsto \pi'_i(m)$; enfin, soit $\zeta_i = \varpi_i \varpi'_i \in \mathrm{End}_A(M_1)$. On a alors :

$$\sum_{i=1}^{s'} \zeta_i = \sum_{i=1}^{s'} \varpi_i \varpi'_i = \sum_{i=1}^{s'} \pi_1 \pi_i|_{M_1} = \pi_1 \,\mathrm{Id}\,|_{M_1} = \mathrm{Id}_{M_1}.$$

Par le corollaire A.11, comme M_1 est indécomposable et que la somme des ζ_i est inversible, il existe j' dans $[1, s']$ tel que $\zeta_{j'}$ est inversible. On en choisit un et l'on pose $\sigma(1) = j'$.

Montrons que M_1 et $M'_{\sigma(1)}$ sont isomorphes. Comme $\zeta_{\sigma(1)} = \varpi_{\sigma(1)} \varpi'_{\sigma(1)}$ est inversible, cela implique que $\varpi_{\sigma(1)}$ est surjective et $\varpi'_{\sigma(1)}$ est injective. Montrons alors que $\varpi_{\sigma(1)}$ est injectif, ce qui donnera le résultat désiré. On voit que $\varpi'_{\sigma(1)} \zeta^{-1}_{\sigma(1)}$ est une section de $\varpi_{\sigma(1)}$. Cela entraîne que $M'_{\sigma(1)}$ se décompose comme somme du noyau de $\varpi_{\sigma(1)}$ et d'un sous-module isomorphe à M_1. Comme $M'_{\sigma(1)}$ est indécomposable, il en résulte que le noyau est nul, d'où l'isomorphisme.

Afin d'achever la preuve du théorème par une récurrence sur s, il suffit de montrer que les quotients M/M_1 et $M/M'_{\sigma(1)}$ sont isomorphes. On vient de voir en fin de compte que π_1 se restreint en un isomorphisme de $M'_{\sigma(1)}$ sur M_1. Cela implique en particulier que l'on a : $\ker(\pi_1) \cap M'_{\sigma(1)} = \{0\}$ et donc, par un argument de dimension : $M = M'_{\sigma(1)} \oplus (M_2 \oplus \cdots \oplus M_s)$. On peut conclure. □

A.15. Exemple. Une matrice diagonale par blocs sur le corps $\mathbb{K}$ dont les blocs diagonaux sont des blocs de Jordan définit un $\mathbb{K}[X]$-module comme

dans II-A. Ce module est indécomposable exactement lorsqu'il n'y a qu'un seul bloc. Le théorème de Krull-Schmidt donne donc la clause d'unicité dans le théorème de Jordan pour les matrices nilpotentes ([H2G2, théorèmes III-2.5]) ou, si $\mathbb{K}$ est algébriquement clos, dans le théorème de la forme normale de Jordan (théorème III-3.3, *op. cit.*).

On en déduit le résultat annoncé.

A.16. Corollaire. *Soit Q un carquois fini et soit V une représentation de Q. Soient $V = \bigoplus_{k=1}^{n} I_k$ et $V = \bigoplus_{k=1}^{n'} I'_k$ deux décompositions de V en somme directe de représentations indécomposables. Alors, on a : $n' = n$ et il existe une permutation σ dans $\mathfrak{S}_n$ telle que $I_{\sigma(k)}$ est isomorphe à I'_k pour tout k.*

Démonstration. Une fois traduit en termes de $\mathbb{K}Q$-modules, c'est le théorème de Krull-Schmidt, qui est valable dans ce cadre puisque les modules sont des espaces de dimension finie. □

A.17. Tirée en arrière et poussée en avant d'une suite exacte

Les résultats qui suivent seront appliqués à l'algèbre des chemins d'un carquois, en identifiant modules sur cette algèbre et représentations de carquois. Toutefois, la construction que nous proposons ici est valable pour toute algèbre associative A sur un corps $\mathbb{K}$. On veut construire de façon naturelle de nouvelles suites exactes à partir d'une suite exacte et d'un morphisme.

Soient quatre A-modules M, M' et L, L'. La composition, ingrédient aussi simple qu'essentiel, définit deux applications $\mathrm{Hom}_A(L,M)\times\mathrm{Hom}_A(L',L) \to \mathrm{Hom}_A(L',M)$ et $\mathrm{Hom}_A(M,M') \times \mathrm{Hom}_A(L,M) \to \mathrm{Hom}_A(L,M')$. On va construire des applications « supérieures » $\mathrm{Ext}^1(L,M) \times \mathrm{Hom}_A(L',L) \to \mathrm{Ext}^1(L',M)$ et $\mathrm{Hom}_A(M,M')\times\mathrm{Ext}^1(L,M) \to \mathrm{Ext}^1(L,M')$. Enfin pas tout à fait sous cette forme, car nous resterons au niveau des suites exactes. Mais par souci de complétude, on précise ensuite le lien entre suites exactes et espaces Ext^1, qui ont été rencontrés en 5.3.

A.17.1. La tirée en arrière

Lemme. *Soit $0 \to M \to E \to L \to 0$ une suite exacte courte et soit $\delta : L' \to L$ un morphisme de A-modules. Il existe une suite exacte, unique à équivalence près, qui complète le diagramme commutatif :*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\iota'} & E' & \xrightarrow{\pi'} & L' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_M} & & \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \delta} & & \\ 0 & \longrightarrow & M & \xrightarrow{\iota} & E & \xrightarrow{\pi} & L & \longrightarrow & 0. \end{array}$$

Définition. La suite exacte du haut dans le lemme est alors appelée *tirée en arrière* de la suite exacte du bas. Si l'on ne craint pas l'anglicisme, on pourra dire aussi *pullback*, qui sonne quand même plus *funky*.

Démonstration. On commence par la construction. On pose :

$$E' = \big\{(e,\ell') \in E \oplus L' \,:\, \pi(e) = \delta(\ell')\big\} \subset E \oplus L',$$
$$\pi'(e,\ell') = \ell', \quad \iota'(m) = (\iota(m),0), \quad \Delta(e,\ell') = e.$$

On vérifie que tout est bien défini, en particulier que $\iota'(m)$ appartient bien à E' pour tout $m \in M$. En effet, on a : $\pi\big(\iota(m)\big) = 0 = \delta(0)$. On identifiera désormais $\iota'(m)$ et $\iota(m)$. On vérifie aussi que E' est bien un A-module et que l'on a défini des morphismes de A-modules. On vérifie sans peine que les deux carrés commutent, c'est-à-dire que $\Delta \circ \iota' = \iota$ et $\delta \circ \pi' = \pi \circ \Delta$.

Reste à voir l'exactitude. On a par construction : $\pi' \circ \iota' = 0$. De plus, si $e' = (e,\ell') \in E'$ appartient au noyau de π', alors : $\ell' = \pi'(e,\ell') = 0$, et donc : $\pi(e) = \delta(0) = 0$. Il vient : $e \in \ker\pi = \mathrm{im}(\iota)$ et donc : $e' = (\iota(m),0) = \iota'(m)$ pour $m \in M$ convenable. Ainsi, $\ker\pi' = \mathrm{im}\,\iota'$. Enfin, pour vérifier l'injectivité de ι' et la surjectivité de π', il suffit de trouver une rétraction[20] pour ι' et une section pour π'. Soient r une rétraction de ι et s une section de π, on pose :

$$r'(e,\ell') = r\big(e\big), \quad \text{et} \quad s'(\ell') = \big(s\big(\delta(\ell')\big),\ell'\big).$$

Vérifions que r' est une rétraction. Pour $m \in M$, on a :

$$r'\big(\iota'(m)\big) = r'\big(\iota(m)\big) = r\big(\iota(m-0)\big) = m.$$

L'application s' va bien dans E' (elle est bien co-définie), car pour tout $\ell' \in L'$, on a : $\pi\big(s\big(\delta(\ell')\big)\big) = \delta(\ell')$; de plus, s' est bien une section

$$\pi'\big(s'(\ell')\big) = \pi'\big(s\big(\delta(\ell')\big) \oplus \ell'\big) = \ell'.$$

Pour l'unicité, supposons avoir un deuxième diagramme :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{\iota_2'} & E_2' & \xrightarrow{\pi_2'} & L' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{Id}_M} & & \downarrow{\scriptstyle \Delta_2} & & \downarrow{\scriptstyle \delta} & & \\
0 & \longrightarrow & M & \xrightarrow{\iota} & E & \xrightarrow{\pi} & L & \longrightarrow & 0.
\end{array}$$

Soit $e_2' \in E_2'$. On a : $\pi\big(\Delta_2(e_2')\big) = \delta\big(\pi_2'(e_2')\big)$ donc $\big(\Delta_2(e_2'),\pi_2'(e_2')\big) \in E'$. On vérifie alors que l'application $\Xi : E_2' \to E'$, $e_2' \mapsto \big(\Delta_2(e_2'),\pi_2'(e_2')\big)$ est

[20] Attention, la section et la rétraction cherchées sont de simples applications linéaires et non des morphismes de A-modules.

un morphisme et fait commuter le diagramme :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\iota'_2} & E'_2 & \xrightarrow{\pi'_2} & L' & \longrightarrow & 0 \\ & & \| & & \downarrow \Xi & & \| & & \\ 0 & \longrightarrow & M & \xrightarrow{\iota'} & E' & \xrightarrow{\pi'} & L' & \longrightarrow & 0, \end{array}$$

ce qui prouve que Ξ est un isomorphisme. D'où l'unicité de la tirée en arrière à équivalence près. □

A.17.2. La poussée en avant

La poussée en avant n'est pas un terme rugbystique mais le dual de la tirée en arrière, et inversement. En conséquence, les flèches sont inversées (pour garder les suites exactes de gauche à droite, on échangera plutôt M et L), et les constructions diffèrent au sens où les sous-espaces deviennent des quotients.

Lemme. *Soit $0 \to M \to E \to L \to 0$ une suite exacte et soit $\gamma : M \to M'$ un morphisme de A-modules. Il existe une suite exacte, unique à équivalence près, qui complète le diagramme commutatif :*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\iota} & E & \xrightarrow{\pi} & L & \longrightarrow & 0 \\ & & \downarrow \gamma & & \downarrow \Gamma & & \downarrow \mathrm{Id}_L & & \\ 0 & \longrightarrow & M' & \xrightarrow{\iota'} & E' & \xrightarrow{\pi'} & L & \longrightarrow & 0. \end{array}$$

Définition. La suite exacte du bas dans A.17.2 est alors appelée *poussée en avant* de la suite exacte du haut. On pourra faire une entorse à la francophonie en lui préférant le terme plus musical de *pushforward*.

Démonstration. On pose :

$$E' = (M' \oplus E)/\{\iota(m) - \gamma(m),\ m \in M\},$$
$$\iota'(m') = \overline{(m', 0)}, \quad \pi'\big(\overline{(m', e)}\big) = \pi(e), \quad \Gamma(e) = \overline{(0, e)},$$

où l'on note $\overline{(m,e)}$ l'image d'un élément (m,e) de $M \oplus E$ dans E'. On vérifie que tout est bien défini, en particulier que π' passe bien au quotient. Cela est vrai car $\pi\iota(m) = 0$ pour tout m de M. On vérifie aussi que E' est bien un A-module, que l'on a défini des morphismes de A-modules, que les deux carrés commutent, et que la suite est exacte. Les preuves sont les « duales » des preuves autour de la construction du *pullback*. □

A.17.3. Extensions

Soient L et M deux modules sur une $\mathbb{K}$-algèbre A. Une *extension* de L par M est un A-module E que l'on peut intégrer à une suite exacte :

$$0 \to M \xrightarrow{\iota} E \xrightarrow{\pi} L \to 0.$$

On choisit une section s de π *comme application linéaire sur* $\mathbb{K}$, de sorte à identifier L à $s(L)$ et ainsi identifier *l'espace vectoriel* E à la somme directe $M \oplus L$. On décrit l'action d'un élément a de A sur E par une matrice :

$$a|_E = \begin{pmatrix} a|_M & z(a) \\ 0 & a|_L \end{pmatrix}.$$

Le zéro en bas à gauche est dû au fait que M est bien un sous-module de E alors que L, *a priori*, non. Ici, l'application z est donc un morphisme linéaire de A dans $\mathrm{Hom}_{\mathbb{K}}(L, M)$.

Espace des cycles. Pour a et a' dans A, la relation $a|_E \circ a'|_E = (aa')|_E$ s'écrit, compte tenu des relations analogues pour L et M :

$$z(aa') = a|_M \circ z(a') + z(a) \circ a'|_L.$$

L'ensemble des morphismes linéaires z de A vers $\mathrm{Hom}_{\mathbb{K}}(L, M)$ qui satisfont à cette relation est noté $Z(L, M)$. Il s'agit donc d'un sous-espace de $\mathrm{Hom}_{\mathbb{K}}\big(A, \mathrm{Hom}_{\mathbb{K}}(L, M)\big)$, appelé, espace des cycles qui décrit les extensions possibles de L par M.

Espace des bords. Cette description est pour l'instant pour le moins grossière et demande à être affinée (comprendre : « quotienter » !) : si z est nul dans $Z(L, M)$, alors le A-module E est la somme directe des modules M et L, mais la réciproque est loin d'être vraie.

En effet, pour φ quelconque dans $\mathrm{Hom}_{\mathbb{K}}(L, M)$, on peut construire un nouvelle action de A sur E en conjuguant l'action de A sur E par l'application linéaire

$$\Phi = \begin{pmatrix} \mathrm{Id}_M & \varphi \\ 0 & \mathrm{Id}_L \end{pmatrix}.$$

Autrement dit, si le A-module E est donné par le morphisme $\alpha : A \to \mathrm{End}(E)$, alors la nouvelle action est donnée par $\alpha' = \Phi^{-1} \circ \alpha \circ \Phi$.

On obtient alors une extension isomorphe à E, c'est-à-dire une extension E' (égale à $E = M \oplus L$ comme espace) telle que l'on ait le diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\iota} & E' & \xrightarrow{\pi} & L & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ & & \mathrm{Id}_M & & \Phi & & \mathrm{Id}_L & & \\ 0 & \longrightarrow & M & \xrightarrow{\iota} & E & \xrightarrow{\pi} & L & \longrightarrow & 0. \end{array}$$

De plus, le petit calcul matriciel suivant donne :

$$\begin{pmatrix} \mathrm{Id}_M & \varphi \\ 0 & \mathrm{Id}_L \end{pmatrix}^{-1} \begin{pmatrix} a|_M & z(a) \\ 0 & a|_L \end{pmatrix} \begin{pmatrix} \mathrm{Id}_M & \varphi \\ 0 & \mathrm{Id}_L \end{pmatrix} = \begin{pmatrix} a|_M & z'(a) \\ 0 & a|_L \end{pmatrix},$$

avec

$$z'(a) = z(a) + b(a) \quad \text{où } b(a) = a|_M \circ \varphi - \varphi \circ a|_L.$$

On note donc $B(L,M)$ l'espace des bords, constitué des applications linéaires $a \mapsto a|_M \circ \varphi - \varphi \circ a|_L$, où φ parcourt $\mathrm{Hom}_{\mathbb{K}}(L,M)$. Par construction[21], $B(L,M)$ est un sous-espace de $Z(L,M)$. On vient donc de voir que deux cycles z et z' de $Z(L,M)$, qui sont égaux modulo $B(L,M)$ définissent deux A-modules isomorphes, l'isomorphisme étant donné par Φ.

Enfin, on définit l'*espace des extensions* de L par M par :

$$\mathrm{Ext}^1_A(L,M) = \mathrm{Ext}^1(L,M) = Z(L,M)/B(L,M).$$

Alors, étant donné un élément ζ de $\mathrm{Ext}^1(L,M)$, on forme une extension bien définie de L par M en choisissant $z \in \mathrm{Hom}_{\mathbb{K}}(L,M)$ qui relève ζ et en définissant l'action de A sur l'espace vectoriel $M \oplus L$ comme ci-dessus. Par exemple, pour $\zeta = 0$, on peut prendre $z = 0$ et l'on retrouve la somme directe $M \oplus L$.

Extensions équivalentes. Inversement, appelons *équivalentes* deux extensions E et E' de L par M s'il existe un morphisme de A-modules $\Xi : E \to E'$ qui fait commuter le diagramme :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{\iota'} & E' & \xrightarrow{\pi'} & L & \longrightarrow & 0 \\
 & & \| & & \downarrow \Xi & & \| & & \\
0 & \longrightarrow & M & \xrightarrow{\iota} & E & \xrightarrow{\pi} & L & \longrightarrow & 0.
\end{array}$$

La condition de commutation du diagramme fait que le morphisme Ξ est nécessairement de la forme de Φ ci-dessus pour $\varphi \in \mathrm{Hom}_{\mathbb{K}}(L,M)$ convenable. On en déduit le résultat qui suit.

A.18. Proposition. *La relation sur les extensions définie ci-dessus est bien une relation d'équivalence. On a une bijection entre classes d'équivalence et éléments de* $\mathrm{Ext}^1(L,M)$.

A.19. Mise en garde. Pour $\zeta \in \mathrm{Ext}^1(L,M)$ et $\lambda \in \mathbb{K}^*$, les extensions définies par ζ et $\lambda\zeta$ ne sont pas équivalentes (sauf si $\lambda = 1$) mais les extensions correspondantes sont des A-modules isomorphes : conjuguer l'endomorphisme $a|_E$ de $M \oplus L$ ci-dessus par $(\lambda \mathrm{Id}_M) \oplus \mathrm{Id}_L$ revient à multiplier $z(a)$ par λ.

[21] On peut poser $z = 0$ et voir que z', qui est un cycle, parcourt $B(L,M)$ quand φ parcourt $\mathrm{Hom}_{\mathbb{K}}(L,M)$. Mais on peut aussi le vérifier par la relation $z(aa') = a|_M \circ z(a') + z(a) \circ a'|_L$ vue plus haut.

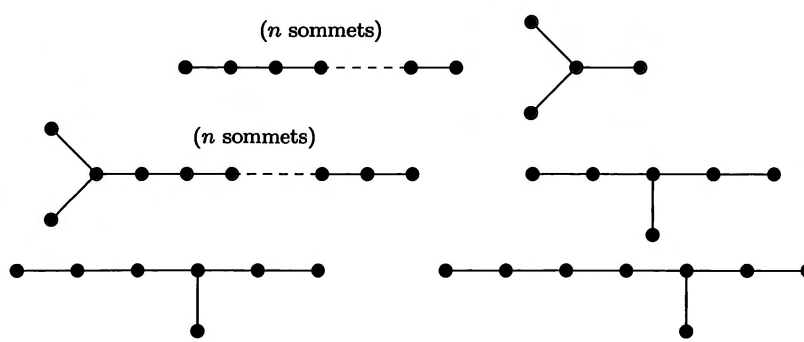
B. Annexe. Graphes dont la forme de Tits est définie positive et graphes étendus

Mystère : les diagrammes de Dynkin se retrouvent dans bon nombre de domaines des mathématiques. Double mystère (quand même lié au premier) : la plupart des preuves qui mènent à eux passent par la célèbre inéquation

$$\frac{1}{p+1}+\frac{1}{q+1}+\frac{1}{r+1}>1 \quad (p,q,r\in\mathbb{N}).$$

Nous allons voir que la classification des graphes dont la forme de Tits associée est définie positive aboutit aux diagrammes de Dynkin et la preuve de ce résultat passe par l'*énigmatique inéquation.* Nous introduirons ensuite les diagrammes de Dynkin affines qui fournissent les graphes dont la forme de Tits associée est positive, mais non définie.

B.1. Définition. On appelle[22] *diagrammes de Dynkin* les graphes suivants : A_n $(n \geqslant 1)$, D_4, D_n $(n \geqslant 5)$, E_6, E_7, E_8, donnés respectivement par :



Un carquois sera dit *de type Dynkin* si les composantes connexes de son graphe non orienté sous-jacent sont des diagrammes de Dynkin.

Le théorème suivant vient compléter la classification du théorème 7.7.

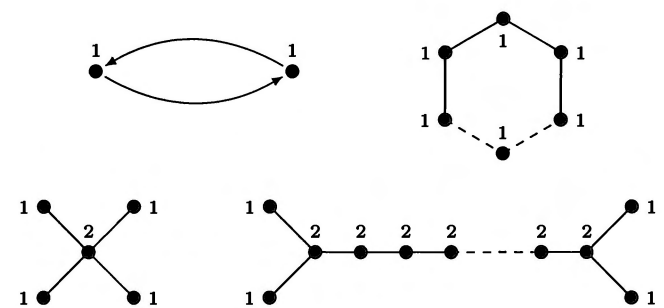
B.2. Théorème. *Soit Q un carquois. La forme de Tits associée à Q est définie positive si et seulement si Q est de type Dynkin.*

Démonstration. On pourra bien sûr se restreindre sans perte de généralité au cas où Q est *connexe.*

[22]Ici, nous fermons les yeux sur quelques familles de diagrammes dits *non simplement lacés* qui n'interviennent pas dans les représentations de carquois sur un corps algébriquement clos. Nous les entrouvrirons au §XI-9.7.

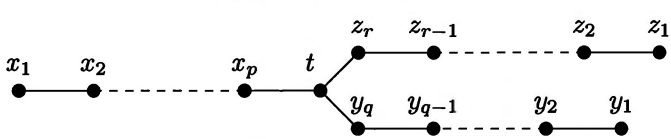
Supposons donc que la forme de Tits q sur $\mathbb{R}^{Q_0}$ associée à Q est définie positive. Alors, en enlevant un ensemble Q_0' de sommets à Q, et en gardant toutes les flèches correspondant aux sommets restants (on dit que l'on considère un sous-carquois *plein*), on obtient un carquois dont la forme de Tits est la restriction de la forme q au sous-espace[23] $\mathbb{R}^{Q_0 \setminus Q_0'}$, donc cette forme de Tits est encore définie positive. De plus, si l'on enlève des flèches, on obtient un carquois dont la forme de Tits est supérieure à q, donc forcément définie positive. Ainsi, en prenant un sous-carquois de Q (on enlève des sommets et des flèches), on obtient encore un carquois dont la forme de Tits est définie positive (sauf pour l'ensemble vide, où certains aimeront trouver des contre-exemples[24]).

Le carquois Q ne peut donc contenir aucun des carquois suivants :



pour lesquels les vecteurs indiqués sur le dessin sont isotropes : $q(1,1) = 0$, $q(1,\ldots,1) = 0$, $q(1,1,2,1,1) = 0$, $q(1,1,2,\ldots,2,1,1) = 0$.

Il n'y a donc ni cycle, ni sommet avec strictement plus de trois voisins, ni strictement plus d'un embranchement : le carquois Q est donc un arbre à trois branches de la forme $Y_{p,q,r}$ $(p,q,r \in \mathbb{N})$:



Pour n entier naturel, soit c_n la forme quadratique définie sur $\mathbb{R}^{n+1}$ par

$$c_n(x_1,\ldots,x_{n+1}) = x_1^2+\cdots+x_n^2+\frac{n}{2(n+1)}x_{n+1}^2-x_1x_2-x_2x_3-\cdots-x_nx_{n+1}.$$

[23] On plonge l'espace $\mathbb{R}^{Q_0 \setminus Q_0'}$ des fonctions de $Q_0 \setminus Q_0'$ dans $\mathbb{R}$ dans l'espace $\mathbb{R}^{Q_0}$ en prolongeant par zéro sur Q_0'.

[24] Toute proposition qui concerne les éléments de l'ensemble vide est vraie. C'est très pratique dans la vie de tous les jours : j'ai pu dire à l'agent Lacroix qui m'a arrêté l'autre jour que je me reposais sur sa capacité de compréhension.

On vérifie par un calcul direct que pour $x \in \mathbb{R}^p$, $y \in \mathbb{R}^q$, $z \in \mathbb{R}^r$, $t \in \mathbb{R}$, on a :

$$\nu(x,y,z,t) = c_p(x_1,\dots,x_p,t) + c_q(y_1,\dots,y_q,t) + c_r(z_1,\dots,z_r,t) + \Big(1 - \frac{p}{2(p+1)} - \frac{q}{2(q+1)} - \frac{r}{2(r+1)}\Big)t^2.$$

De plus, pour tout $n \in \mathbb{N}$, c_n est une forme positive et son noyau est la droite engendrée par $(1,2,\dots,n+1)$. Cela provient de l'égalité, pour $x \in \mathbb{R}^n$:

$$c_n = \sum_{i=1}^{n} \frac{i}{2(i+1)} \Big(x_{i+1} - \frac{i+1}{i} x_i\Big)^2.$$

On voit donc que ν est positive.

Montrons que ν est définie positive si et seulement si

$$1 - \frac{p}{2(p+1)} - \frac{q}{2(q+1)} - \frac{r}{2(r+1)} > 0.$$

En effet, si l'inégalité n'est pas satisfaite, on choisit $v^{(n)} \in \mathbb{R}^n$ tel que $(v^{(n)},1)$ engendre le noyau de c_n et l'on calcule :

$$\nu(v^{(p)},v^{(q)},v^{(r)},1) = 0 + \Big(1 - \frac{p}{2(p+1)} - \frac{q}{2(q+1)} - \frac{r}{2(r+1)}\Big) \leqslant 0,$$

donc ν n'est pas définie positive. Réciproquement, si l'inégalité est satisfaite, alors la relation $\nu(x,y,z,t) = 0$ implique que l'on a :

$$c_p(x_1,\dots,x_p,t) = c_q(y_1,\dots,y_q,t) = c_r(z_1,\dots,z_r,t) = t = 0.$$

Vu la description du noyau de c_n, il vient : $(x,y,z,t) = 0$.

Or, en écrivant $-p/(p+1) = -1 + 1/(p+1)$, on transforme cette inégalité en l'*énigmatique inéquation*, caractérisant le fait que ν est définie positive :

$$\frac{1}{p+1} + \frac{1}{q+1} + \frac{1}{r+1} > 1.$$

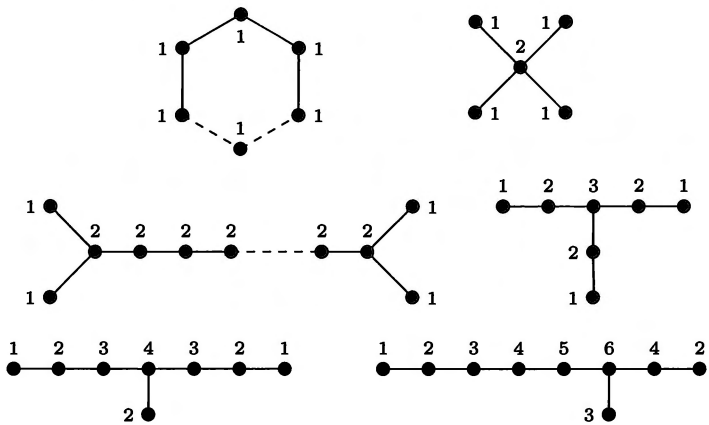
Résolvons-la. Par symétrie, quitte à permuter les variables p, q et r, on peut supposer que l'on a $p \leqslant q \leqslant r$. On vérifie qu'il n'y a pas de solution avec $p \geqslant 2$. Si $p = 0$, alors $(0,q,r)$ est solution pour tout (q,r). Si $p = q = 1$, alors $(1,1,r)$ est solution pour tout r. Si $p = 1$ et $q \geqslant 3$, il n'y a pas de solution. Si $p = 1$ et $q = 2$, on vérifie que les seules valeurs possibles pour r sont 2, 3 et 4. En définitive, toute solution (p,q,r) dans $\mathbb{N}^3$ est l'une des suivantes :

(i) $(0,q,r)$ $((q,r) \in \mathbb{N}\times\mathbb{N})$, ce qui donne le graphe A_n avec $n = q+r+1$;
(ii) $(1,1,r)$ $(r \in \mathbb{N}^*)$ ce qui donne le graphe D_n avec $n = r+3$;
(iii) $(1,2,2)$, ce qui donne le graphe E_6 ;
(iv) $(1,2,3)$, ce qui donne le graphe E_7 ;
(v) $(1,2,4)$, ce qui donne le graphe E_8.

Réciproquement, le calcul de ν en fonction des c_n montre que tous les diagrammes de Dynkin sont associés à des formes de Tits définies positives. Pour une preuve alternative de cette réciproque, voir le lemme XI-9.4. □

B.3. Remarque. On retrouvera cette inéquation en IX-2.5.

B.4. Définition. Les *diagrammes de Dynkin affines* sont les graphes $\tilde{A}_n$ ($n \geqslant 1$), $\tilde{D}_4$, $\tilde{D}_n$ ($n \geqslant 4$), $\tilde{E}_6$, $\tilde{E}_7$, $\tilde{E}_8$, donnés respectivement par :



Un carquois sera dit *de type Dynkin affine* si les composante connexes du graphe non orienté sous-jacent sont des diagrammes de Dynkin affines.

B.5. Notations. Les nombres placés sur les sommets ne correspondent pas ici à une numérotation fantasque et insensée, mais ils donnent un générateur entier de la droite isotrope de la forme de Tits correspondante. Plus précisément, le générateur en question est donné par $(n_i)_{i \in Q_0} \in \mathbb{Z}^{Q_0}$, où n_i est le nombre associé au sommet i dans le graphe.

La preuve du théorème suivant est esquissée en exercice.

B.6. Théorème. *Soit Q un carquois. La forme de Tits associée à Q est positive non définie si et seulement si Q est de type Dynkin affine.*

B.7. Exercice (Esquisse de preuve). *Soit Q un carquois, que l'on peut supposer connexe, de forme de Tits associée positive (et non définie).*

1. *Montrer que Q ne peut pas contenir strictement :*
   (a) une boucle ;
   (b) un cycle (sans être lui-même un cycle) ;
   (c) un sommet attaché à cinq autres sommets ;
   (d) trois sommets attachés à deux sommets.

   Pour chaque cas, on exhibe, par l'absurde, un vecteur dont l'image par la forme de Tits est dans $\mathbb{R}^{-*}$.

2. *Montrer que si un sommet est attaché à quatre autres sommets, alors le graphe est $\tilde{D}_4$.*

   Il le contient et l'on montre qu'il ne peut le contenir strictement en faisant partir une flèche d'un sommet. Il faudra faire plusieurs cas selon la source et le but de la flèche.

3. *Montrer que si deux sommets sont attachés à trois sommets, alors Q est de type $\tilde{D}_n$.*

   Même méthode. Plusieurs cas sont à prévoir également.

4. *Si l'on n'est pas en type $\tilde{D}_n$, montrer que si un sommet est attaché à trois sommets, alors, ce sommet est unique.*

5. *En déduire que si le graphe n'est ni de type $\tilde{A}_n$, ni de type $\tilde{D}_n$, il est de type $Y_{p,q,r}$, avec cette fois-ci $(p+1)^{-1}+(q+1)^{-1}+(r+1)^{-1}=1$.*

6. *Résoudre cette équation et obtenir les derniers graphes $\tilde{E}_6$, $\tilde{E}_7$, $\tilde{E}_8$.*

C. Annexe. Théorème du rang constant

C.1. Théorème (du rang constant). *Soient f une application différentiable définie sur un ouvert W de $\mathbb{R}^n$ dans $\mathbb{R}^m$ et a dans W. On suppose que la différentielle de f est de rang constant r sur W. Il existe alors :*

- *un voisinage ouvert V_1 de $f(a)$,*
- *un difféomorphisme φ de V_1 vers un voisinage ouvert W' de 0 dans $\mathbb{R}^n$ qui envoie $f(a)$ sur 0,*
- *un voisinage ouvert $W_1 \subset W$ de a,*
- *un difféomorphisme ψ de W_1 vers un voisinage ouvert W' de 0 dans $\mathbb{R}^n$ qui envoie a sur 0,*

tels que

$$\varphi \circ f \circ \psi^{-1}(y_1,\dots,y_n) = (y_1,\dots,y_r,0,\dots,0)$$

pour $(y_1,\dots,y_n) \in W'$.

Pour faire simple, le théorème dit que, localement et à changement de coordonnées près, une application de rang constant r peut être vue comme la projection standard de $\mathbb{R}^n$ sur $\mathbb{R}^r$ suivie de l'injection de $\mathbb{R}^r$ dans $\mathbb{R}^m$.

Remarquons que si f est linéaire, c'est exactement le théorème du rang : il existe des isomorphismes linéaires φ et ψ tels que

$$\varphi f \psi^{-1}(y_1,\dots,y_n) = (y_1,\dots,y_r,0,\dots,0)\,.$$

La preuve consiste d'ailleurs à exploiter cela au point a, puis à l'étendre au voisinage de a.

Démonstration. On peut supposer que $a = 0 \in \mathbb{R}^n$, que $f(a) = 0 \in \mathbb{R}^m$ et que la matrice jacobienne de f en a est

$$\mathrm{I}_{m,n;r} = \begin{pmatrix} \mathrm{I}_r & 0 \\ 0 & 0 \end{pmatrix}.$$

En effet, soit A la matrice de $\mathrm{d}f_a$. Le théorème du rang permet de trouver deux matrices inversibles P et Q telles que $QAP^{-1} = \mathrm{I}_{m,n;r}$.

Notons $q : \mathbb{R}^m \to \mathbb{R}^m$ et $p : \mathbb{R}^n \to \mathbb{R}^n$ les isomorphismes linéaires ayant pour matrices Q et P dans les bases canoniques. Soit $W_1 = p(W - a)$, c'est un ouvert contenant a. Pour $h \in W_1$, posons :

$$\tilde{f}(h) = q\Big(f\big(a + p^{-1}(h)\big) - f(a)\Big),$$

de sorte que $\tilde{f} = \tilde{\varphi} \circ f \circ \tilde{\psi}^{-1}$, où $\tilde{\psi} : x \mapsto p(x-a)$ est un difféomorphisme de W sur W_1 et $\tilde{\varphi} : y \mapsto q\big(y - f(a)\big)$ est un difféomorphisme de $\mathbb{R}^m$ sur $\mathbb{R}^m$. Il suffit de prouver le théorème pour $\tilde{f}$ pour le déduire pour f. Or, on a : $\tilde{f}(0) = 0$ et $\mathrm{d}\tilde{f}_0 = q \circ \mathrm{d}f_a \circ p^{-1}$, qui a pour matrice $\mathrm{I}_{m,n;r}$, ce qui permet d'ajouter les hypothèses du début de la preuve.

Pour $x = (x_j)_{1 \leqslant j \leqslant n} \in W$, écrivons :

$$f\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 + g_1(x_1, \ldots, x_n) \\ \vdots \\ x_r + g_r(x_1, \ldots, x_n) \\ g_{r+1}(x_1, \ldots, x_n) \\ \vdots \\ g_m(x_1, \ldots, x_n) \end{pmatrix}.$$

Par hypothèse, la matrice de $\mathrm{d}f_0$ est $\mathrm{I}_{m,n;r}$, de sorte que les dérivées partielles des g_i s'annulent toutes en 0. Posons alors :

$$\psi\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 + g_1(x_1, \ldots, x_n) \\ \vdots \\ x_r + g_r(x_1, \ldots, x_n) \\ x_{r+1} \\ \vdots \\ x_m \end{pmatrix}.$$

Comme les dérivées partielles des g_i s'annulent en 0, la différentielle de ψ en 0 est l'identité. Par suite, ψ se restreint en un difféomorphisme d'un voisinage $W_1 \subset W$ de 0 sur $W' = \psi(W_1)$. On peut supposer W_1 et W' connexes.

Soit $h_i = g_i \circ \psi^{-1} : W' \to \mathbb{R}$ si $r+1 \leqslant i \leqslant m$. Pour $y = (y_j)_{1 \leqslant j \leqslant n} \in W'$, on a :

$$f \circ \psi^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_r \\ h_{r+1}(y_1, \ldots, y_n) \\ \vdots \\ h_m(y_1, \ldots, y_r) \end{pmatrix}.$$

Comme la différentielle de ψ^{-1} est un isomorphisme linéaire en tout point de W', la matrice jacobienne de $f \circ \psi^{-1}$ est de rang constant égal à r. Le point clé, c'est que ses r premières lignes forment en tout point la sous-matrice $(\mathrm{I}_r \; 0)$: comme elle est déjà de rang r, le bloc inférieur droit est partout nul ! Autrement dit, comme fonctions sur W', on a :

$$\forall i \geqslant r+1, \; \forall j \geqslant r+1, \quad \frac{\partial h_i}{\partial y_j} = 0.$$

Par connexité de W', cela entraîne que $h_{r+1}, \ldots, h_r$ ne dépendent pas de $y_{r+1}, \ldots, y_n$: on les définit comme des fonctions sur $U_1 = U \subset \mathbb{R}^r$, où U est l'ouvert des $(y_1, \ldots, y_r)$ tels que $(y_1, \ldots, y_r, 0, \ldots, 0) \in W'$. Enfin, on définit une application sur le voisinage $V_1 = U_1 \times \mathbb{R}^{m-r}$ de $0 \in \mathbb{R}^m$ par :

$$\varphi \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_r \\ z_{r+1} - h_{r+1}(z_1, \ldots, z_r) \\ \vdots \\ z_m - h_m(z_1, \ldots, z_r) \end{pmatrix},$$

qui est manifestement un difféomorphisme de V_1 sur $V' = V_1$ (son inverse s'obtient en remplaçant h_i par $-h_i$). On a finalement, pour $y \in W'$:

$$\varphi \circ f \circ \psi^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_r \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

ce qui prouve le théorème. □

Voici le corollaire dont nous aurons besoin pour étendre le « théorème de submersion » [H2G2, théorème IX-A.11].

C.2. Corollaire. *Soit U un ouvert de $\mathbb{R}^n$ et soit φ une application différentiable de $\mathbb{R}^n$ dans $\mathbb{R}^m$ dont la différentielle est de rang constant sur U. Alors, pour tout y dans l'image de φ, l'image réciproque $\varphi^{-1}(y)$ est une sous-variété de U de dimension $n-r$ et le sous-espace tangent en $x \in \varphi^{-1}(y)$ est égal à* $\ker \mathrm{d}_x\varphi$.

Démonstration. Soit x dans $\varphi^{-1}(y)$. Il suffit de montrer qu'il existe un voisinage ouvert $O \subset U$ de x tel que $O \cap \varphi^{-1}(y)$ soit une sous-variété de O. Par le théorème, il suffit de montrer que c'est le cas pour la projection canonique π de $\mathbb{R}^n$ sur $\mathbb{R}^r$. Mais cela est une conséquence du « théorème de submersion » [H2G2, §IX-A.11]. □

C.3. Mise en garde. Localement, tout se passe bien, puisque l'on voit qu'il existe un ouvert $O \subset U$ de x tel que $\varphi(O)$ est une sous-variété. Mais, globalement, les choses peuvent se dégrader, puisque rien ne dit qu'il existe un ouvert O' de $\varphi(x)$ tel que $O' \cap \varphi(U) = O' \cap \varphi(V)$. Et dans ce cas, il peut arriver que l'image $\varphi(U)$ ne soit pas une sous-variété.

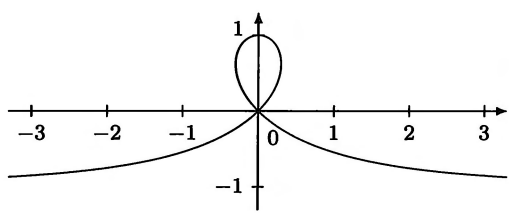


Figure C.1. *Strophoïde droite, image de* $\varphi : t \mapsto \left(\frac{t-t^3}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$

Par exemple, la strophoïde droite de la figure C.1 n'est pas une sous-variété de $\mathbb{R}^2$ alors que la différentielle de l'application dont elle est l'image admet un rang constant égal à 1.

D. Annexe. Polynômes à n indéterminées et topologie

Voici quelques résultats utiles dès que l'on doit gérer des propriétés topologiques de parties de $\mathbb{C}^n$ (muni de sa topologie normique) définies par l'annulation (ou non annulation) de polynômes à n indéterminées sur $\mathbb{C}$. Ils ne sauraient remplacer les résultats de géométrie algébrique nécessaires à la preuve de l'injectivité de **dim** dans le théorème 7.7. Mais ces derniers, pour être prouvés rigoureusement, nécessiteraient l'introduction de toute une théorie et de ses détails, dont on sait que le diable s'y cache.

En avant pour un grand classique. On fixe un entier n et des indéterminées $X_1, \ldots, X_n$.

D.1. Proposition. *Si un polynôme P de $\mathbb{C}[X_1,\dots,X_n]$ s'annule sur un ouvert non vide de $\mathbb{C}^n$, alors P est le polynôme nul : $P=0$.*

Démonstration. On procède par récurrence sur n. Pour $n=1$, c'est une reformulation du fait qu'un polynôme n'a qu'un nombre fini de zéros. Soit n supérieur ou égal à 2, supposons la propriété vraie jusqu'en dimension $n-1$ et supposons qu'il existe Q non constant dans $\mathbb{C}[X_1,\dots,X_n]$ qui s'annule sur un ouvert non vide Ω de $\mathbb{C}^n$. On écrit $Q=\sum_{k=0}^{d} g_k X_n^k$ où les g_k sont des polynômes en $X_1,\dots,X_{n-1}$. Soit $x=(x_1,\dots,x_n)$ un point de Ω : comme il est ouvert, Ω contient un voisinage de x de la forme $\Omega'\times D$, où Ω' est un ouvert de $\mathbb{C}^{n-1}$ et D un disque ouvert de $\mathbb{C}$. Pour $x'\in\Omega'$ (fixé), le polynôme $\sum_{k=0}^{d} g_k(x')X_n^k \in \mathbb{C}[X_n]$ admet une infinité de racines (tous les points de D) : c'est donc le polynôme nul. Par suite, tous les g_k s'annulent sur Ω'. Par hypothèse de récurrence, ces polynômes sont tous nuls, ce qui permet de conclure. □

Ce corollaire n'a rien à voir avec les problèmes de ce chapitre, mais il illustre bien l'utilité de la proposition.

D.2. Corollaire (Cayley-Hamilton). *Soit A une matrice complexe carrée et χ_A son polynôme caractéristique. Alors, on a : $\chi_A(A)=0$.*

Démonstration. Les coefficients du polynôme caractéristique de A sont des polynômes en les coefficients de A. Pour tout polynôme P, les coefficients de la matrice $P(A)$ sont des polynômes en les coefficients de P et en ceux de A. Ainsi, les coefficients de $\chi_A(A)$ sont des polynômes en les coefficients de A. Plus précisément, le choix d'une base de l'espace des matrices permet d'écrire l'application $\mathscr{M}_n(\mathbb{K})\to\mathscr{M}_n(\mathbb{K})$, $A\mapsto\chi_A(A)$ sous la forme $(x_{ij})_{1\leqslant i,j\leqslant n}\mapsto\big(P_{k\ell}(x_{ij})\big)_{1\leqslant k,\ell\leqslant n}$, où les $P_{k\ell}$ sont des polynômes en n^2 variables.

Or, chacun de ces polynômes $P_{k\ell}$ s'annule sur l'ensemble non vide des matrices à spectre simple, qui est le complémentaire du fermé défini par l'équation polynomiale : $\mathrm{Res}(\chi_A,\chi_A')=0$. Ici, Res désigne le *résultant* — autrement dit, $\mathrm{Res}(\chi_A,\chi_A')$ est le *discriminant* du polynôme $A\mapsto\chi_A$. Comme le discriminant est un polynôme non nul, ce complémentaire contient un ouvert non vide. La proposition D.1 permet de conclure : tous les coefficients $P_{k\ell}$ de $\chi_A(A)$ sont nuls. □

D.3. Remarque. Comme la preuve de [H2G2, proposition II-2.2.4], cette preuve ne parle que du corps des complexes. Mais pour étendre le théorème de $\mathbb{C}$ à tout corps (et même tout anneau !), il suffit de remarquer que les $P_{k\ell}$ appartiennent à $\mathbb{Z}[X_{ij}]$ et qu'ils sont *indépendants de* $\mathbb{K}$. En effet, le déterminant est un polynôme à coefficients entiers indépendant du corps,

de même que les coefficients de la somme et du produit de deux matrices. Ainsi, dire que les $P_{k\ell}$ sont nuls comme polynômes, c'est dire que $\chi_A(A) = 0$ pour toute matrice A sur tout corps $\mathbb{K}$.

Mais, revenons aux propriétés topologiques liées aux polynômes.

D.4. Proposition. *Soit* $V = \{x \in \mathbb{C}^n,\ P(x) \neq 0\}$, *où* P *est un polynôme non nul de* $\mathbb{C}[X_1, \ldots, X_n]$. *Alors,* V *est dense dans* $\mathbb{C}^n$.

Démonstration. Si $n = 1$, le résultat est vrai car V est alors égal à $\mathbb{C}$ privé d'un nombre fini de points. Prenons n quelconque. Si V n'est pas $\mathbb{C}^n$ entier, fixons x hors de V et montrons que tout voisinage ouvert de x rencontre V.

Supposons au contraire qu'il existe une boule centrée en x qui n'intersecte pas V. Pour tout u dans $\mathbb{C}^n$, on considère le polynôme $Q_u = P(x + uT) \in \mathbb{C}[T]$. Comme Q_u s'annule sur un voisinage de 0, c'est le polynôme nul. Donc P s'annule sur toute la droite $\{x+ut,\ t \in \mathbb{C}\}$ et ce, pour tout u. Cela signifie que P est le polynôme nul. Absurbe. □

D.5. Corollaire. *Soient* s *et* t *entiers et soient* $(P_i)_{1 \leqslant i \leqslant s}$ *et* $(Q_j)_{1 \leqslant j \leqslant t}$ *deux familles de polynômes non nuls de* $\mathbb{C}[X_1, \ldots, X_n]$. *Soit alors*

$$V = \{x \in \mathbb{C}^n,\ P_i(x) \neq 0, Q_j(x) = 0, \forall i, j\}.$$

Si V *contient un ouvert de* $\mathbb{C}^n$, *alors* $t = 0$ *et* V *est dense dans* $\mathbb{C}^n$.

Démonstration. Par hypothèse, les Q_j sont des polynômes non nuls qui s'annulent sur un ouvert. D'après la proposition D.1, on a bien : $t = 0$. D'après la proposition D.4, V est alors une intersection d'ouverts denses ; il est donc dense. □

E. Exercices du chapitre III

Algèbres de chemins, A-modules

E.1. Exercice. *Soit Q un carquois fini. Montrer que la dimension de $\mathbb{K}Q$ est finie si et seulement si Q ne possède pas de cycles orientés.*

E.2. Exercice. *Soit A une $\mathbb{K}$-algèbre et soit une suite exacte de A-modules*

$$0 \longrightarrow M \xrightarrow{\iota} E \xrightarrow{\pi} L \longrightarrow 0.$$

1. *Montrer que pour tout A-module X, l'application $f \mapsto \iota \circ f$ définit une injection de $\mathrm{Hom}_A(X,M)$ dans $\mathrm{Hom}_A(X,E)$.*
2. *Montrer que si un élément g de $\mathrm{Hom}_A(X,E)$ satisfait à $\pi \circ g = 0$, alors g se factorise par ι.*
3. *En déduire que l'on a la suite exacte suivante :*

$$0 \longrightarrow \mathrm{Hom}_A(X,M) \xrightarrow{\iota\circ ?} \mathrm{Hom}_A(X,E) \xrightarrow{\pi\circ ?} \mathrm{Hom}_A(X,L).$$

4. *Pour l'algèbre des chemins du carquois A_2, voir l'exemple 4.5, avec*

$$0 \longrightarrow S_2 \xrightarrow{\iota} P_1 \xrightarrow{\pi} S_1 \longrightarrow 0,$$

montrer que $\mathrm{Hom}_{\mathbb{K}Q}(S_1,S_2)=0$, $\mathrm{Hom}_{\mathbb{K}Q}(S_1,P_1)=0$, $\mathrm{Hom}_{\mathbb{K}Q}(S_1,S_1)=\mathbb{K}$ et en déduire que $\pi\circ ?$ n'est en général pas surjective.

5. *Montrer de façon duale que la suite suivante est exacte :*

$$0 \longrightarrow \mathrm{Hom}_A(L,X) \xrightarrow{?\circ\iota} \mathrm{Hom}_A(E,X) \xrightarrow{?\circ\pi} \mathrm{Hom}_A(M,X).$$

E.3. Exercice (Modules projectifs et idempotents)

Soit A un anneau. Un A-module P est dit projectif, *si pour toute suite exacte de A-modules $M \xrightarrow{\pi} N \to 0$ et tout morphisme $\phi : P \to N$, il existe un morphisme $\psi : P \to M$ tel que $\pi\psi = \phi$. On se propose de montrer des propriétés élémentaires des modules projectifs.*

1. *Montrer qu'un A-module libre de type fini est projectif.*
   Prendre une base du module libre et définir ψ sur une base.
2. *Montrer que P est un module projectif si et seulement si P est facteur direct d'un module libre.*
   « Si » : utiliser le fait qu'un morphisme partant de P se prolonge en un morphisme partant du module libre $L = P \oplus M$. « Seulement si » : on construit un morphisme surjectif $\pi : A^n \to P$ à partir d'un système à n générateurs du A-module. L'identité de P, qui est projectif, permet de fournir une section pour π. On peut injecter P dans A^n qui a alors pour supplémentaire le noyau.

3. *Montrer qu'un module P cyclique,* i.e. *engendré par un seul élément, est projectif si et seulement si $P \simeq Ae$, pour un idempotent e de A.*
« Si » : on a $A = Ae \oplus A(1-e)$. « Seulement si » : on construit une surjection $\pi : A \to P$ avec $a = p(1)$ un générateur. Soit σ une section pour π, posons $e = s(a)$. On a $e^2 = e\sigma\big(\pi(1)\big) = \sigma\big(\pi(e)\big) = \sigma(a) = e$.

E.4. Exercice. *Soit A la $\mathbb{K}$-algèbre des chemins d'un carquois et soit M un A-module. Soit i un sommet du carquois et soit $e_i \in A$ le chemin paresseux correspondant, comme dans la définition A.2. Montrer que l'on a un isomorphisme de $\mathbb{K}$-espaces :*

$$\mathrm{Hom}_A(Ae_i, M) \to e_iM.$$

Envoyer le morphisme ϕ sur $\phi(e_i) = e_i\phi(e_i) \in e_iM$. Réciproquement, pour e_im dans e_iM, construire le morphisme qui envoie ae_i ($a \in A$) vers ae_im.

E.5. Exercice. *On reprend les notations de l'exercice E.4. Le but de l'exercice est de montrer que le module Ae_i est un module indécomposable. On suppose donc $Ae_i = M_1 \oplus M_2$ une décomposition en A-modules, et l'on veut montrer que $M_1 = 0$ ou $M_2 = 0$.*

1. *Soit π la projection de Ae_i sur M_1 selon M_2. On a bien sûr : $\pi \in \mathrm{Hom}_A(Ae_i, Ae_i)$. Montrer qu'il existe $f \in e_iAe_i$ tel que $\pi(x) = xf$ pour tout x de Ae_i.*
C'est l'application immédiate de l'exercice E.4 en posant $M = Ae_i$.
2. *Montrer que f vérifie alors $f(f - e_i) = 0$.*
Comme π est un projecteur, on a $f^2 = f = fe_i$.
3. *En déduire que $f = 0$ ou $f = e_i$.*
On pourra d'abord montrer que si $0 \neq x \in Ae_i$ et $0 \neq y \in e_iA$, alors $xy \neq 0$. Pour ce faire, on peut considérer dans la décomposition de x et y en chemins, des chemins de longueur maximale.
4. *Conclure.*

E.6. Exercice. *On reprend les notations de l'exercice E.4. Le but de l'exercice est de montrer que si i et j sont des sommets distincts, alors $Ae_i \not\simeq Ae_j$. On pourra donc conclure avec les exercices précédents que le A-module libre A se décompose en somme directe sans multiplicité, des A-modules projectifs indécomposables Ae_i. On suppose donc donnés des isomorphismes inverses l'un de l'autre $\varphi : Ae_i \to Ae_j$ et $\psi : Ae_j \to Ae_i$ et donc, par l'exercice E.4, deux éléments correspondants respectivement aux morphismes φ et ψ : $f \in e_iAe_j$ et $g \in e_jAe_i$.*

1. *Montrer que $fg = e_i$ et que $gf = e_j$.*
Cela ne fait qu'exprimer le fait que φ et ψ sont inverses l'un de l'autre.
2. *En déduire $e_j \in Ae_iA$, puis que $j = i$.*

E.7. Exercice (*Joke:* le théorème de la base incomplète confirmé !)

La théorie des carquois permet de donner une preuve raffinée au théorème de la base incomplète. On considère le carquois Q formé d'un seul sommet (sans flèche).

1. *Montrer que la forme de Tits est donnée par $q_Q(x) = x^2$, que l'algèbre de chemins est $\mathbb{K}Q = \mathbb{K}$ sur un corps quelconque $\mathbb{K}$.*
2. *En déduire que pour tout couple (M, N) de $\mathbb{K}$-espace vectoriels, on a : $[M, N]^1 = 0$.*
3. *En déduire que tout sous-espace d'un espace E possède un supplémentaire.*
   C'est le corollaire 5.6.

Extensions. Ordre de dégénérescence

E.8. Exercice (Propriété d'élimination de l'ordre de dégénérescence)

On travaille sur $\mathbb{C}$. Soient V, W, Z des représentations du carquois Q et soient f un endomorphisme de la représentation Z et $g \in \mathrm{Hom}_{\mathbb{K}Q}(Z, Y)$. On veut montrer que si W est le conoyau de $\begin{pmatrix} f & g \end{pmatrix}$, c'est-à-dire si l'on a la suite exacte

$$0 \longrightarrow Z \xrightarrow{(f\ g)} Z \oplus Y \xrightarrow{\pi} W \longrightarrow 0$$

alors, on a : $W \leqslant_{\deg} Y$.

1. *Montrer que si $f - \lambda \mathrm{Id}_Z$ est un automorphisme de Z, alors l'application naturelle de Y sur $\mathrm{Coker}\begin{pmatrix} f - \lambda \mathrm{Id}_Z & g \end{pmatrix}$ est un isomorphisme.*
2. *En déduire que $W \leqslant_{\mathrm{hom}} Z$.*
   Ça ne fait pas avancer le problème que l'on a posé au départ, mais ce n'est pas difficile à montrer vu que la dimension du conoyau est, à l'instar de celle du noyau, semi-continue supérieurement.
3. *Montrer que si une famille d'applications linéaires surjectives $\varphi_\lambda \in \mathrm{Hom}_{\mathbb{K}}(E, F)$, indexée par $\lambda \in \mathbb{C}^*$, converge en $\lambda = 0$ vers une application linéaire surjective φ, alors on peut trouver une famille de sections (linéaires !) s_λ de φ_λ convergeant vers une section de φ.*
   On pourra raisonner matriciellement et faire un réarrangement de lignes pour visualiser une sous-matrice carrée inversible.
4. *En déduire que $W \leqslant_{\deg} Z$.*
   Le morphisme de représentations $Z \oplus Y \to W$ est constitué, pour chaque sommet, d'applications linéaires surjectives. C'est un bon début.

Les travaux de Klaus Bongartz et Grzegorz Zwara ont permis de montrer, avec des hypothèses très larges, que l'on a équivalence entre $W \leqslant_{\deg} Y$ et l'existence d'un Z et d'une suite exacte comme ci-dessus. C'est le théorème d'annulation qui constitue une belle caractérisation de la dégénérescence d'orbites via la théorie des représentations.

E.9. Exercice (Somme de deux extensions)

Soit Q un carquois fini. On rappelle que si L et M sont des $\mathbb{K}Q$-modules, ou de façon équivalente, des représentations de Q, on a défini à partir de $\mathrm{Ext}^1(L,M) = Z(L,M)/B(L,M)$ *une classe d'équivalence d'extensions*

$$0 \longrightarrow M \xrightarrow{\iota} E \xrightarrow{\pi} L \longrightarrow 0.$$

Comme $\mathrm{Ext}^1(L,M)$ *est un groupe additif, on aimerait fournir, en terme de suites exactes, la construction de la somme de deux extensions. Soient donc $\varphi, \gamma \in \mathrm{Ext}^1(L,M)$, que l'on relève en des éléments respectifs f et g de $Z(L,M)$.*

1. *Soient E_φ et E_γ des extensions associées respectivement à φ et γ. Construire une suite exacte naturelle*

$$0 \longrightarrow M \oplus M \longrightarrow E_\varphi \oplus E_\gamma \longrightarrow L \oplus L \longrightarrow 0,$$

et donner la matrice de l'action d'une flèche $\alpha \in Q_1$ sur $E_\varphi \oplus E_\gamma$.

2. *Construire le* pullback *de la suite précédente, puis le* pushforward *de la suite obtenue, comme dans le diagramme*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M \oplus M & \longrightarrow & E_\varphi \oplus E_\gamma & \longrightarrow & L \oplus L & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \mathrm{Id}_{M\oplus M}} & & \uparrow & & \uparrow{\scriptstyle \binom{\mathrm{Id}_L}{\mathrm{Id}_L}} & & \\
0 & \longrightarrow & M \oplus M & \longrightarrow & E & \longrightarrow & L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle (\mathrm{Id}_M \ \mathrm{Id}_M)} & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}_L} & & \\
0 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & L & \longrightarrow & 0.
\end{array}$$

Montrer que la représentation E' ainsi construite est bien une extension $E_{\varphi+\gamma}$ de L par M correspondant à la somme $\varphi + \gamma$.
On considère l'extension intermédiaire E définie par $\binom{a}{b} \in Z(L, M\oplus M)$ et l'extension E' définie par $c \in Z(L,M)$. On utilise le fait que les flèches $E \to E_\varphi \oplus E_\gamma$ et $E \to E'$ sont des morphismes de représentations pour obtenir, pour tout $\alpha \in Q_1$ les égalités

$$\begin{pmatrix} \mathrm{Id}_M & & 0 \\ & \mathrm{Id}_M & 0 \\ 0 & & \mathrm{Id}_L \\ & 0 & \mathrm{Id}_L \end{pmatrix} \begin{pmatrix} M_\alpha & & a(\alpha) \\ & M_\alpha & b(a) \\ 0 & 0 & L_\alpha \end{pmatrix} = \begin{pmatrix} M_\alpha & & f(\alpha) & \\ & M_\alpha & & g(\alpha) \\ 0 & & L_\alpha & \\ & 0 & & L_\alpha \end{pmatrix} \begin{pmatrix} \mathrm{Id}_M & & 0 \\ & \mathrm{Id}_M & 0 \\ & & \mathrm{Id}_L \\ 0 & 0 & \mathrm{Id}_L \end{pmatrix},$$

$$\begin{pmatrix} \mathrm{Id}_M & \mathrm{Id}_M & 0 \\ 0 & 0 & \mathrm{Id}_L \end{pmatrix} \begin{pmatrix} M_\alpha & & f(\alpha) \\ & M_\alpha & g(\alpha) \\ 0 & 0 & L_\alpha \end{pmatrix} = \begin{pmatrix} M_\alpha & c(\alpha) \\ 0 & L_\alpha \end{pmatrix} \begin{pmatrix} \mathrm{Id}_M & \mathrm{Id}_M & 0 \\ 0 & 0 & \mathrm{Id}_L \end{pmatrix},$$

et en déduire $c(\alpha) = f(\alpha) + g(\alpha)$.

E.10. Exercice (Produit d'un scalaire par une extension)

Comme dans l'exercice précédent, on note E_φ (la classe d'isomorphisme de) l'extension de L par M correspondant à $\varphi \in \mathrm{Ext}^1(L,M)$.

1. *Soi $t\lambda \in \mathbb{K}^*$. Montrer que les suites exactes associées à E_φ et à $E_{\lambda\varphi}$ sont équivalentes.*
   On peut considérer l'application linéaire de E_φ dans $E_{\lambda\varphi}$ qui s'écrit matriciellement dans une base adaptée $\begin{pmatrix} \mathrm{Id}_M & 0 \\ 0 & \lambda^{-1}\mathrm{Id}_L \end{pmatrix}$ et montrer qu'elle commute à l'action d'une flèche $\alpha \in Q_1$.
2. *Montrer qu'il existe une application surjective ε qui envoie un élément de $\mathbb{P}\,\mathrm{Ext}^1(L,M)$ vers une classe d'extension non scindée de L par M.*
3. *Montrer qu'en général, l'application ε n'est pas injective.*
   Il n'est pas la peine d'aller chercher bien loin. On prend le carquois de type A_2 : $1 \longrightarrow 2$, $M : 0 \to \mathbb{C}$, $L : \mathbb{C}^2 \to 0$. ce qui donne, par le théorème de Gabriel (ou sans !), deux classes d'extensions de vecteur de dimension $(2,1)$, une scindée et une non scindée. En particulier, $\mathrm{Ext}^1(L,M)$ est non nul et donc $|\mathbb{P}\,\mathrm{Ext}^1(L,M)| > 1$. L'application ne peut être injective.

Classification, théorème de Gabriel

E.11. Exercice (Paires de drapeaux et permutations)

On explicite dans un cas particulier la bijection de la proposition 8.10. On fait agir $\mathrm{GL}_n(\mathbb{C})$ naturellement sur le produit $\mathscr{B} \times \mathscr{B}$ de la variété des drapeaux complets de $\mathbb{C}^n$ avec elle-même. On considère donc le carquois Q

$$\overset{1}{\bullet} \longrightarrow \overset{2}{\bullet} \longrightarrow \cdots \longrightarrow \overset{n-1}{\bullet} \longrightarrow \overset{n}{\bullet} \longleftarrow \overset{n-1}{\bullet} \longleftarrow \cdots \longleftarrow \overset{2}{\bullet} \longleftarrow \overset{1}{\bullet}$$

et le vecteur de dimension $\mathbf{d}$ indiqué sur les sommets du carquois. On numérote les sommets du carquois de droite à gauche par $Q_0 = \{1,2,3,\ldots,n,n+1,\ldots,2n-2,2n-1\}$. On veut expliciter une bijection $V \mapsto w_V$ qui envoie une classe de représentation V de $\mathrm{Rep}^0_{\mathbf{d}}/G_{\mathbf{d}}$ vers un élément w_V de $\mathscr{B}\times\mathscr{B}/\mathrm{GL}_n = \mathfrak{S}_n$, voir exercice I-C.18. Pour tout couple (i,j) de $[1,n]$, on note $V^{i,j}$ la représentation indécomposable de Q déterminée par $V^{i,j}_k = \mathbb{C}$ pour $i \leqslant k \leqslant 2n-j$ et $V^{i,j}_k = 0$ sinon.

1. *Soit V une représentation de $\mathrm{Rep}^0_{\mathbf{d}}$. Montrer qu'il existe $w = w_V \in \mathfrak{S}_n$ tel que V est isomorphe $\bigoplus_{i=1}^n V^{i,w(i)}$.*
   La classification des indécomposables et l'injectivité des flèches implique que toute représentation indécomposable de la décomposition est de la forme $V^{i,j}$. En considérant le vecteur de dimension $\mathbf{d}$, on voit qu'il existe un unique indécomposable de la forme $V^{1,w(1)}$, puis par récurrence, un unique indécomposable de la forme $V^{k,w(k)}$, pour tout k

de $[1,n]$. L'égalité $\mathbf{dim}\, V = \mathbf{d}$ implique alors que w est surjective de $[1,n]$ dans $[1,n]$. Donc, bijective.

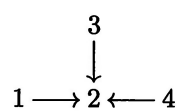
2. *Comparer, via la bijection établie l'ordre de Bruhat de W et l'ordre de dégénérescence de $\mathrm{Rep}_{\mathbf{d}}^0/G_{\mathbf{d}} \simeq W$.*
   Les ordres sont les mêmes. Utiliser successivement le corollaire 8.15 et la dernière question de l'exercice I-C.18.
3. *Montrer par récurrence sur l'ordre de Bruhat que la « dimension » de l'orbite (dans le sens de la remarque 6.7) correspondant à $w \in W$ est égale à la longueur $\ell(w)$ de w.*
   La comparaison peut se faire par récurrence à l'aide du calcul de la codimension de l'orbite associée à la représentation V donnée par $[V,V]^1 = [V,V]^0 - q(V)$, d'une part, et le calcul de la longueur donnée par la proposition I-A.11, d'autre part.

E.12. Exercice. *Soit Q un carquois de type $A-D-E$ et soit X une représentation de Q. On suppose que M est une sous-représentation indécomposable de X et que $X/M \simeq M$. Montrer que $X \simeq M \oplus M$.*

Par le lemme de Ringel, la formule 4.14, on a : $\mathrm{Ext}^1(M,M) = 0$. Par le corollaire 5.6, toute suite exacte $0 \to M \to X \to M \to 0$ est donc scindée.

Carquois et géométrie

E.13. Exercice. *Sachant que trois droites en position générale dans le plan projectif se coupent en trois points non alignés, trouver l'orbite ouverte du carquois de type D_4*

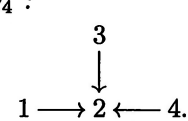


pour le vecteur de dimension $(2,3,2,2)$.

Si l'on note M_{ij}, $i,j \neq 2$ la représentation indécomposable où $\mathbb{C}$ est placé sur les sommets i, j et 2. Alors, il s'agit de la représentation $M_{13} \oplus M_{14} \oplus M_{34}$.

E.14. Exercice. *On considère trois droites en position générale dans $\mathbb{P}^3(\mathbb{C})$. On veut montrer avec les représentations de carquois qu'il existe une famille de droites sécantes à ces trois droites paramétrée par $\mathbb{P}^1(\mathbb{C})$; une sécante commune est représentée sur la figure E.1.*

Soit Q le carquois de type D_4 :



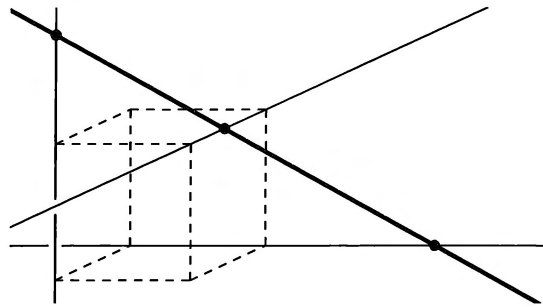


Figure E.1. *Une sécante commune à trois droites en position générale*

1. *Montrer que les trois droites en position générale dans* $\mathbb{P}^3(\mathbb{C})$ *correspondent, en les relevant dans* $\mathbb{C}^4$*, à une représentation* X *de* Q *de vecteur de dimension* $\mathbf{d} = (2,4,2,2)$ *telle que l'orbite associée soit ouverte et dense.*
   En prenant les images de chaque flèche comme dans le lemme 8.3, on voit que trois plans dans $\mathbb{R}^4$ correspondent à une représentation de vecteur de dimension $\mathbf{d}$. Comme Q est de type fini, il y a une unique orbite ouverte et dense en toute dimension, en particulier en dimension $\mathbf{d}$, correspondant à ce que l'on peut nommer « position générale ».
2. *Soit* M *l'unique représentation indécomposable de vecteur de dimension* $(1,2,1,1)$*. Montrer que* $X \simeq M \oplus M$*.*
   Il suffit, par unicité de l'orbite dense, d'établir que $[M \oplus M, M \oplus M]^1 = 0$, sachant que $[M,M]^1 = 0$. Cela se démontre par exemple en utilisant $[M \oplus M, M \oplus M]^0 = 4[M,M]^0$ ainsi que la formule 4.14.
3. *Montrer que l'ensemble des droites sécantes aux trois droites est en bijection avec* $\mathrm{Hom}_Q(M,X)^0/\mathrm{Aut}(M)$*, où* $\mathrm{Hom}_Q(M,X)^0$ *est l'ouvert des morphismes injectifs de* M *dans* X *et où* $\mathrm{Aut}(M)$ *agit naturellement à droite.*
   Écrire le diagramme commutatif de flèches injectives correspondant à une injection ι de M dans X et voir qu'une droite sécante correspond à l'image de ι.
4. *Conclure.*
   On a : $\mathrm{Hom}_Q(M,X)^0/\mathrm{Aut}(M) \simeq \mathbb{P}^1$, car M étant indécomposable, $\mathrm{Hom}_Q(M,M) = \mathbb{R}$.

On remarquera que tous les résultats sont encore valables sur $\mathbb{R}$.

Among the maxims on Lord Naoshige's wall,
there was this one : "Matters of great concern should be treated lightly"
Master Ittei commented, "Matters of small concern should be treated seriously".
Jim Jarmusch, *Ghost Dog : The Way of the Samurai*, 1999.

Chapitre IV

Combinatoire algébrique

Le dénombrement représente toujours un défi à notre connaissance. Au-delà de l'utilité immédiate que l'on pourrait en tirer, comme établir une bijection par exemple, savoir compter les objets dont nous disposons, c'est se prouver que l'on est bien le maître de notre domaine.

Comme dans [H2G2, chapitre VIII], nous allons donc dénombrer tout ce qui bouge, dans le riche contexte de la géométrie des corps finis, faisant ainsi ce que l'on appelle communément de la « combinatoire quantique ». Cette appellation n'est pas innocente ; elle nous aide à penser ce travail comme un analogue de la combinatoire classique. En effet, si l'on considère naïvement que la combinatoire classique voit les cardinaux comme somme d'unités, la combinatoire quantique voit de son côté les cardinaux d'objets sur $\mathbb{F}_q$ comme somme de q^n, c'est-à-dire, comme polynômes à coefficients entiers positifs en q. Or, q^n est le cardinal de l'espace affine de dimension n, qui devient, dans ce contexte, l'unité, ou disons, la cellule.

Toute l'idée est donc de décomposer les objets à étudier (grassmanniennes, variétés des drapeaux) en réunion d'espaces affines disjoints.

On notera au passage la remarquable analogie classique/quantique, où l'ensemble $E = \{1, \dots, n\}$, l'ensemble $\mathscr{P}(E)$ des parties de E et l'ensemble $\mathscr{P}^m(E)$ des parties de E à m éléments correspondent respectivement à l'espace projectif $\mathbb{P}^n(\mathbb{F}_q)$, la variété des drapeaux complets $\mathscr{B}$ et à la grassmannienne $\mathrm{Gr}_{m,n}(\mathbb{F}_q)$ des sous-espaces de dimension m de $\mathbb{F}_q^n$. Par analogue quantique (ou *q-analogue*), on entend que l'on retrouve les résultats du cas classique en posant $q = 1$ dans les polynômes en q obtenus.

Ainsi, la décomposition en cellules de la grassmannienne décrite au chapitre I permet d'obtenir une expression polynomiale pleine de charme pour $|\mathrm{Gr}_{m,n}(\mathbb{F}_q)|$, qui par la suite fournit le q-analogue de la formule du binôme

de Newton, ou *q-binôme*. L'introduction de séries génératrices, idée dont l'efficacité est déjà éprouvée, donne la *formule du triple produit de Jacobi*. On en profite pour quelques batifolages autour des *nombres pentagonaux d'Euler*.

Plus loin, on prolonge le travail commencé dans [H2G2, chapitre VIII] sur le calcul de l'ordre des groupes classiques sur les corps finis. L'objet de la partie suivante est donc de calculer l'ordre des groupes orthogonaux sur les corps finis. On sait classifier les formes quadratiques sur un corps fini à l'aide du discriminant. On obtient alors deux groupes orthogonaux essentiels, dont on se propose de calculer l'ordre.

Pour cela, on utilise le théorème de Witt ou, disons, un corollaire direct : la transitivité de l'action de ces groupes sur les nappes quadratiques ne contenant pas 0. On donne, comme application, le calcul du cardinal d'une nappe quadratique, c'est-à-dire, finalement, le nombre de solutions, dans $\mathbb{F}_q^n$, d'une équation homogène de degré 2.

On peut alors revenir sur le cardinal des grassmanniennes, mais cette fois-ci, on étudie les grassmanniennes et les variétés des drapeaux de sous-espaces totalement isotropes (SETI) de dimension donnée. Encore une fois, la transitivité l'action du groupe orthogonal, due au théorème de Witt, permettra de résoudre le problème.

Pour clore ce chapitre, on calculera le cardinal du cône des matrices nilpotentes de $\mathscr{M}_n(\mathbb{F}_q)$. Ce sera l'occasion de voir à l'œuvre les techniques de type « désingularisation », déjà introduites dans le chapitre II. Mais la beauté ne réside pas cette fois uniquement dans le chemin : le résultat est aussi fascinant qu'inattendu. En effet, le cardinal du cône nilpotent est celui d'un espace affine (ou vectoriel), alors que l'objet est tout de même assez loin d'être un espace.

La fin de cette histoire est hors de portée de l'ouvrage. Cette coïncidence numérique indique que le cône nilpotent complexe (si !) a les mêmes invariants topologiques qu'un espace affine (ceux fournis par la « cohomologie ℓ-adique », pour être précis). Cela peut être vu par les fans de médailles Fields comme une invitation aux travaux de Grothendieck et Deligne sur les conjectures de Weil.

1. Grassmannienne et formule du binôme quantique

Never send a human to do a machine's job.
Andy & Larry Wachowski, *The Matrix*, 2003.

Le but de cette partie est de déduire de la décomposition en cellules de la grassmannienne la formule combinatoire connue sous le nom de « binôme quantique » et d'en tirer quelques conséquences. On rappelle tout d'abord quelques résultats de [H2G2, proposition VIII-1.1] sur les cardinaux de l'espace projectif, la variété des drapeaux (complets) et les grassmanniennes sur un corps fini. Ces calculs reposaient sur la description d'actions transitives de groupes appropriés et des stabilisateurs d'éléments particuliers.

1.1. Proposition. *Soit q une puissance d'un nombre premier et soient m et n des entiers naturels tels que $0 \leqslant m \leqslant n$. On a :*

$$\left|\mathbb{P}^{n-1}(\mathbb{F}_q)\right| = 1+q+q^2+\cdots+q^{n-1}, \quad \left|\mathscr{F}_n(\mathbb{F}_q)\right| = \prod_{k=1}^{n}(1+q+\cdots+q^{k-1})$$

$$\left|\operatorname{Gr}_{m,n}(\mathbb{F}_q)\right| = \frac{\displaystyle\prod_{k=1}^{n}(1+q+\cdots+q^{k-1})}{\displaystyle\prod_{k=1}^{m}(1+q+\cdots+q^{k-1})\prod_{k=1}^{n-m}(1+q+\cdots+q^{k-1})}.$$

On adopte donc les notations suivantes, à rapprocher des notations de la combinatoire classique.

1.2. Définition. Soit q une puissance d'un nombre premier ou une indéterminée. Pour n entier naturel, on appelle respectivement *analogue quantique* (ou *q-analogue*) de n et *q-factorielle* de n les polynômes suivants :

$$[n]_q = \left|\mathbb{P}^{n-1}(\mathbb{F}_q)\right| = 1+q+q^2+\cdots+q^{n-1}$$

$$\text{et} \quad [n]_q! = \left|\mathscr{F}_n(\mathbb{F}_q)\right| = \prod_{k=1}^{n}(1+q+\cdots+q^{k-1}).$$

(Pour $n=0$, on convient de prendre $[0]_q = 0$ et $[0]_q! = 1$.)

Pour m et n entiers naturels tels que $0 \leqslant m \leqslant n$, on appelle *$q$-coefficient binomial* le polynôme

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \left|\operatorname{Gr}_{m,n}(\mathbb{F}_q)\right| = \frac{[n]_q!}{[m]_q![n-m]_q!}.$$

Lorsque n est un entier strictement négatif ou que l'inégalité $0 \leqslant m \leqslant n$

n'est pas satisfaite, on convient que

$$[n]_q! = 0 \ (n < 0), \quad \begin{bmatrix} n \\ m \end{bmatrix}_q = 0 \ (m < 0 \text{ ou } n < m).$$

On rappelle la décomposition en cellules de la grassmannienne — voir [H2G2, théorème IV-3.2.4].

1.3. Théorème. *Soit $\mathbb{K}$ un corps. Soient m et n deux entiers tels que $0 \leqslant m \leqslant n$. La grassmannienne est la réunion disjointe*

$$\mathrm{Gr}_{m,n}(\mathbb{K}) = \bigcup_{\mathbf{i}=(1\leqslant i_1<i_2<\cdots<i_m\leqslant n)} \mathscr{O}_{\mathbf{i}},$$

où $\mathscr{O}_{\mathbf{i}}$ est en bijection avec l'espace vectoriel $\mathbb{K}^{|\mathbf{i}|}$, et $|\mathbf{i}| = \sum_{j=1}^{m}(i_j - j)$.

Pour rappel, $\mathscr{O}_{\mathbf{i}}$ est l'ensemble des matrices de $\mathscr{M}_{n,m}$ qui se réduisent par action à droite de $\mathrm{GL}_m(\mathbb{K})$ en une matrice co-échelonnée réduite de type $\mathbf{i}$. Voir [H2G2, définition IV-3.2.1] pour la définition d'une matrice co-échelonnée réduite.

1.4. Exemple. Voici une matrice co-échelonnée réduite de type $(2,3,5)$:

$$\begin{pmatrix} * & * & * \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & * \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

où les $*$ représentent des scalaires quelconques. Chaque colonne admet un unique pivot (le coefficient non nul le plus bas, qui vaut 1) et des zéros en dessous et à droite de chaque pivot. On voit bien sur cet exemple que l'ensemble des matrices de $\mathscr{M}_{6,3}$ co-échelonnées réduites de type $(2,3,5)$ est en bijection avec $\mathbb{K}^d$ avec $d = (2-1) + (3-2) + (5-3) = 4$.

Si l'on travaille maintenant sur un corps fini $\mathbb{K} = \mathbb{F}_q$, on peut comparer les cardinaux des deux ensembles. Celui de gauche est dans la proposition 1.1, celui de droite est clair. On obtient :

$$\frac{(q^n-1)(q^{n-1}-1)\times\cdots\times(q^{n-m+1}-1)}{(q^m-1)(q^{m-1}-1)\times\cdots\times(q-1)} = \sum_{\mathbf{i}=(1\leqslant i_1<i_2<\cdots<i_m\leqslant n)} q^{|\mathbf{i}|}.$$

1.5. Corollaire. *Soient m et n deux entiers avec $1 \leqslant m \leqslant n$ et soit q une puissance d'un nombre premier. Alors :*

$$\frac{(q^n-1)(q^{n-1}-1)\times\cdots\times(q^{n-m+1}-1)}{(q^m-1)(q^{m-1}-1)\times\cdots\times(q-1)} = \\ = \sum_{1\leqslant i_1<\cdots<i_m\leqslant n} q^{(i_1-1)+(i_2-2)+\cdots+(i_m-m)}.$$

Comme q peut prendre une infinité de valeurs, on peut voir cette égalité comme une identité entre une fraction rationnelle et un polynôme que l'on spécialise (évalue) en q.

En particulier, la fraction rationnelle en q donnée par $\left|\mathrm{Gr}_{m,n}(\mathbb{F}_q)\right|$ se trouve être en réalité un polynôme dont la valeur en $q=1$ est le nombre binomial $\binom{n}{m}$.

1.6. Définition. La polynomialité de ces q-analogues (et le fait qu'il existe une infinité de puissances de nombres premiers) permet d'étendre les définitions 1.2 au cas où q est *une indéterminée* ou un nombre, réel ou complexe.

1.7. Remarque (q générique). Ces q-analogues ne représentent plus grand-chose si q n'est pas la puissance d'un nombre premier : du moins, ce n'est pas le cardinal d'un ensemble aussi naturellement défini qu'un espace projectif fini ou une grassmannienne finie.

Et pourtant... Les topologues avertis reconnaissent dans ce polynôme, qui compte les points de la grassmannienne sur un corps fini, la fonction génératrice d'invariants de la grassmannienne complexe ! C'est un des exemples qui ont poussé Weil à énoncer ses célèbres conjectures, en 1949 dans [83], qui ont été un puissant moteur pour la géométrie algébrique.

1.8. Remarque (« Le corps à un élément »). Il est étonnant de constater que la variable q déjà utilisée par Gauss lui-même et liée au cardinal des corps finis puisse aussi évoquer la déformation quantique chère aux physiciens, au sens suivant. Soit $\hbar$ la constante de Planck et[1] $q=\exp(\hbar)$. Passer à la limite classique, pour un physicien, consiste (en schématisant) à faire tendre $\hbar$ vers 0, c'est-à-dire q vers 1. Or on a :

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\times\cdots\times(q^{n-m+1}-1)}{(q^m-1)(q^{m-1}-1)\times\cdots\times(q-1)} \quad \text{et} \quad \lim_{q\to 1} \begin{bmatrix} n \\ m \end{bmatrix}_q = \binom{n}{m}.$$

On peut imaginer qu'en posant $q=1$ dans ces expressions polynomiales, on interprète n comme le nombre de points de l'espace projectif de dimension $n-1$ sur le « corps à un élément $\mathbb{F}_1$ », ce qui encore une fois ne veut

[1] Que Gauss ait été visionnaire jusque dans les notations, cela tient du prodige.

pas dire grand-chose. De même, dire que le coefficient binomial quantique se spécialise bien en le coefficient binomial classique lorsque $q = 1$, cela suggère que l'analogue d'un sous-espace vectoriel de dimension m sur $\mathbb{F}_1$ dans l'espace $\mathbb{F}_1^n$ est... une partie à m éléments de $\{1, \dots, n\}$.

Étonnamment, la poursuite du « corps à un élément » est un problème actuel de géométrie algébrique.

Voici maintenant, à titre d'exemple, quelques formules de ce que l'on pourrait appeler la « combinatoire quantique ». On introduit une autre indéterminée t pour former des séries génératrices.

1.9. Proposition (Binôme quantique). *On a l'identité :*

$$\sum_{m=0}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_q q^{m(m+1)/2}\, t^m = \prod_{i=1}^{n} (1 + q^i t).$$

Démonstration. Dans le membre de droite de la relation de 1.5, regroupons les puissances négatives de q, ce qui donne un facteur $q^{-m(m+1)/2}$. Multiplions les deux membres par $q^{m(m+1)/2}$:

$$q^{m(m+1)/2} \begin{bmatrix} n \\ m \end{bmatrix}_q = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n} q^{i_1 + i_2 + \cdots + i_m}.$$

Multiplions par t^m pour garder une trace du degré, puis sommons[2] sur m. On obtient :

$$\sum_{m=0}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_q q^{m(m+1)/2}\, t^m = \sum_{m=0}^{n} \sum_{1 \leqslant i_1 < \cdots < i_m \leqslant n} q^{i_1} t\, q^{i_2} t \cdots q^{i_m} t = \prod_{i=1}^{n} (1 + q^i t).$$

□

L'exercice A.11 propose une preuve alternative, par récurrence. Notons que cette formule est un q-analogue de la formule du binôme car, si l'on pose $q = 1$, on retrouve la formule de Newton. On la doit, semble-t-il, à Cauchy, de même que la dérivation suivante de la célèbre formule du *triple produit de Jacobi*, qui nous a été expliquée par Jiang Zeng.

1.10. Proposition (Triple produit de Jacobi)

$$\prod_{m=1}^{+\infty} (1 - q^m)(1 + q^m t^{-1})(1 + q^{m-1} t) = \sum_{j \in \mathbb{Z}} q^{j(j-1)/2}\, t^j.$$

[2] C'est encore là l'idée remarquable des *séries génératrices*, adaptée ici aux q-coefficients binomiaux.

Démonstration. Substituons $q^{-1}t$ à la place de t dans la formule de la proposition 1.9 et réarrangeons, il vient :

$$\prod_{i=1}^{n}(1+q^{i-1}t) = \sum_{m=0}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_q q^{m(m+1)/2} q^{-m} t^m;$$

$$\prod_{i=0}^{n-1}(1+q^{i}t) = \sum_{m=0}^{n} \begin{bmatrix} n \\ m \end{bmatrix}_q q^{m(m-1)/2} t^m.$$

Remplaçons n par $2n$ puis recentrons la variable de sommation ($j = m-n$) :

$$\begin{aligned}\prod_{i=0}^{2n-1}(1+q^{i}t) &= \sum_{m=0}^{2n} \begin{bmatrix} 2n \\ m \end{bmatrix}_q q^{m(m-1)/2} t^m \\ &= \sum_{j=-n}^{n} \begin{bmatrix} 2n \\ n+j \end{bmatrix}_q q^{(n+j)(n+j-1)/2} t^{n+j}.\end{aligned}$$

Prenons $q^{-n}t$ à la place de t :

$$\begin{aligned}\prod_{i=0}^{2n-1}(1+q^{i-n}t) &= \sum_{j=-n}^{n} \begin{bmatrix} 2n \\ n+j \end{bmatrix}_q q^{(n+j)(n+j-1)/2} q^{-n(n+j)} t^{n+j} \\ &= \sum_{j=-n}^{n} \begin{bmatrix} 2n \\ n+j \end{bmatrix}_q q^{j(j-1)/2} q^{-n(n+1)/2} t^n t^j.\end{aligned}$$

Dans le produit, séparons puissances positives et négatives de q :

$$\begin{aligned}\prod_{i=0}^{2n-1}(1+q^{i-n}t) &= \prod_{i=0}^{n-1}(1+q^{i-n}t) \times \prod_{i=n}^{2n-1}(1+q^{i-n}t) \\ &= \prod_{m=1}^{n}(1+q^{-m}t) \times \prod_{\ell=0}^{n-1}(1+q^{\ell}t) \\ &= q^{-n(n+1)/2} t^n \prod_{m=1}^{n}(q^m t^{-1}+1) \times \prod_{\ell=0}^{n-1}(1+q^{\ell}t).\end{aligned}$$

Simplifions à présent par $q^{-n(n+1)/2}t^n$, ce qui donne :

$$\prod_{m=1}^{n}(1+q^m t^{-1})(1+q^{m-1}t) = \sum_{j=-n}^{n} \begin{bmatrix} 2n \\ n+j \end{bmatrix}_q q^{j(j-1)/2} t^j.$$

Passons à la limite $n \to +\infty$ sans nous soucier des problèmes de convergence. La permutation de la limite et de la somme peut être justifiée par un argument formel ou en prenant q complexe de module < 1 et en invo-

quant le théorème de convergence dominée. En revenant à la définition du q-binôme, il vient, à j fixé :

$$\lim_{n\to+\infty}\begin{bmatrix}2n\\ n+j\end{bmatrix}_q = \lim_{n\to+\infty}\frac{\prod_{i=1}^{2n}(1-q^i)}{\prod_{i=1}^{n+j}(1-q^i)\prod_{i=1}^{n-j}(1-q^i)}$$
$$= \frac{\prod_{i=1}^{+\infty}(1-q^i)}{\prod_{i=1}^{+\infty}(1-q^i)\prod_{i=1}^{+\infty}(1-q^i)} = \frac{1}{\prod_{i=1}^{+\infty}(1-q^i)}.$$

D'où finalement, modulo justification de l'interversion $\lim_\infty \sum_j = \sum_j \lim_\infty$, la formule du triple produit de Jacobi. □

Cette formule remarquable possède de nombreuses applications, notamment au dénombrement des partitions et au nombre de décompositions d'un nombre en somme de deux ou quatre carrés, voir par exemple [24], exercice 7.13 et §7.3–7.5. Pour en comprendre le lien, on constate que si l'on fait la substitution q en q^2 et t en tq, on obtient

$$\prod_{m=1}^{+\infty}(1-q^{2m})(1+q^{2m-1}t^{-1})(1+q^{2m-1}t) = \sum_{j\in\mathbb{Z}} q^{j^2}t^j.$$

De plus, en remplaçant q par $q^{3/2}$ et t par $-q^{-1/2}$ dans cette dernière formule, on montre le *théorème du nombre pentagonal d'Euler* :

$$\prod_{n=1}^{\infty}(1-q^n) = \sum_{j\in\mathbb{Z}}(-1)^j q^{\frac{1}{2}j(3j-1)}.$$

On vérifie par récurrence que le nombre $j(3j-1)/2$ est le j-ème *nombre pentagonal* (voir la figure 1.1 et calculer une série arithmétique).

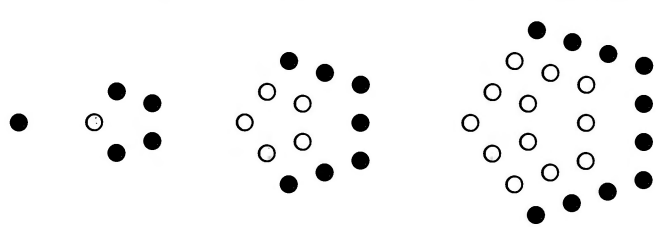


Figure 1.1. *Premiers nombres pentagonaux :* 1, 5, 12, 22...

2. Ordre des groupes orthogonaux sur un corps fini

On a montré que sur un corps fini, le groupe spécial orthogonal en dimension 2 est un groupe cyclique dont il est facile de calculer l'ordre. Le groupe orthogonal est donc, toujours en dimension 2, un groupe diédral. Le but de cette partie est d'explorer le cas des dimensions supérieures. Là, les groupes obtenus sont loin d'être cycliques ou diédraux. Pour en convaincre par un argument d'autorité, nous « rappelons » que les groupes projectifs $\mathrm{PSO}(\mathbb{F}_q)$ contiennent un groupe simple (non cyclique) d'indice 1 ou 2. Nous allons donc nous contenter de calculer l'ordre des groupes orthogonaux sur les corps finis. Pour cela, on se ramène comme d'habitude aux groupes orthogonaux qui stabilisent une forme quadratique non dégénérée. Il existe à isomorphisme près deux groupes orthogonaux de la forme suivante :

$$\mathrm{O}^\zeta(n,\mathbb{F}_q) = \{M \in \mathscr{M}_n(\mathbb{F}_q),\ M\mathrm{I}_\zeta\, {}^tM = \mathrm{I}_\zeta\},$$

où I_ζ est la matrice diagonale $\mathrm{diag}(1,1,\dots,1,\zeta)$, $\zeta \in \mathbb{F}_q^*$. En effet, d'après la classification des formes quadratiques non dégénérées sur les corps finis, il existe à isomorphisme près deux groupes de cette forme selon que ζ est un carré ou non dans $\mathbb{F}_q$. En fait, il existe *au plus* deux groupes orthogonaux, car deux stabilisateurs d'orbites distinctes pourraient bien être isomorphes.

Nous allons voir que l'ordre $\mathfrak{o}_n^\zeta$ du groupe $\mathrm{O}^\zeta(n,\mathbb{F}_q)$ dépend des deux entiers $\varepsilon = \zeta^{(q-1)/2} \in \{1,-1\}$ et $\alpha = (-1)^{(q-1)/2} \in \{1,-1\}$.

2.1. Théorème. *L'ordre $\mathfrak{o}_n^\zeta$ du groupe orthogonal $\mathrm{O}^\zeta(n,\mathbb{F}_q)$ est donné par*

$$\mathfrak{o}_{2n+1}^\zeta = 2q^n \prod_{k=0}^{n-1}(q^{2n}-q^{2k}), \quad \mathfrak{o}_{2n}^\zeta = 2(q^n - \varepsilon\alpha^n)\prod_{k=1}^{n-1}(q^{2n}-q^{2k}).$$

2.2. Remarque. Le lecteur coutumier des groupes de Lie semi-simples complexes ne sera pas surpris de voir ainsi différenciés les cas pair et impair puisque, dans ce contexte, on associe des diagrammes de Dynkin distincts selon la parité. En revanche, le néophyte pourra être surpris de cette distinction. Voici une façon de l'expliquer : pour toute forme quadratique non dégénérée, on a une décomposition de l'espace en une somme directe de plans hyperboliques et d'un sous-espace anisotrope, ce sous-espace étant unique à isométrie près. Quand on travaille sur les corps finis, ce dernier sous-espace est de dimension 0, 1, ou 2. Cela montre que dans le cas impair, il n'y a qu'une seule possibilité (la dimension est 1) et dans le cas pair, il y en a deux selon que le sous-espace non isotrope est de dimension 0 ou 2.

Il est désormais clair qu'en dimension paire, les deux groupes orthogonaux ne sont pas isomorphes puisqu'ils n'ont pas le même ordre selon que ε vaut 1

ou -1. En dimension impaire, l'argument tombe... Arrêtons là le suspens, ils sont bien isomorphes, comme on le verra plus tard.

La preuve que nous donnons du théorème est valable pour toute puissance q d'un nombre premier p. Le lecteur non familier avec les corps finis peut lire cette preuve en supposant que $p = q$.

L'idée de la preuve est de faire agir le groupe orthogonal transitivement (théorème de Witt, [H2G2, théorème V-3.4, corollaire V-3.5]) sur une nappe quadratique bien sentie dont on sait calculer le cardinal ; on montre ensuite que son stabilisateur est (isomorphe à) un groupe orthogonal en dimension inférieure et l'on obtient ainsi une formule de récurrence sur les ordres.

2.3. Notations. Selon la parité de la dimension, nous nous intéresserons à deux types de nappes quadratiques indexées par $a \in \mathbb{F}_q^*$:

$$M_n^a = \{(x_1, x_2, \dots, x_{2n+1}),\ x_1x_2 + \cdots + x_{2n-1}x_{2n} + ax_{2n+1}^2 = 1\} \subset \mathbb{F}_q^{2n+1},$$
$$N_n^a = \{(x_1, \dots, x_{2n}),\ x_1x_2 + \cdots + x_{2n-3}x_{2n-2} + x_{2n-1}^2 + ax_{2n}^2 = 1\} \subset \mathbb{F}_q^{2n}.$$

2.4. Lemme. *Avec les notations précédentes, on a :*

$$|M_n^a| = q^n\big(q^n + a^{\frac{q-1}{2}}\big), \quad |N_n^a| = q^{n-1}\big(q^n - (-a)^{\frac{q-1}{2}}\big).$$

Démonstration (du lemme). Calculons $|M_n^a|$. On fixe à cet effet un n-uplet $(x_1, x_3, \dots, x_{2n-1})$. Pour mémoire, $a^{(a-1)/2}$ est égal au symbole de Legendre, [H2G2, annexe V-C] : il vaut 1 si a est un carré et -1 sinon.

Si l'on a : $(x_1, x_3, \dots, x_{2n-1}) = (0, \dots, 0)$, alors il n'y a aucun point dans la nappe si a n'est pas un carré et $2q^n$ points si a est un carré, ce qui se résume en $q^n(1 + a^{(q-1)/2})$ points.

Si $(x_1, x_3, \dots, x_{2n-1}) \neq (0, \dots, 0)$, alors à chaque choix de x_{2n+1}, les points de M_n^a sont en bijection naturelle avec un hyperplan dans un espace de dimension n (les coordonnées paires). Le nombre de points est alors $q \times q^{n-1}$. Cela fait au total $q^n(1 + a^{(q-1)/2}) + (q^n - 1) \times q \times q^{n-1} = q^n(q^n + a^{(q-1)/2})$ comme annoncé.

À présent, calculons $|N_n^a|$. La même méthode donne :

$$|N_n^a| = q^{n-1}|W_a| + (q^{n-1} - 1)q^2q^{n-2},$$

où W_a est la nappe quadratique en dimension 2 définie par

$$W_a = \{(X, Y),\ X^2 + aY^2 = 1\} \subset \mathbb{F}_q^2.$$

Il reste à montrer que $|W_a| = q - (-a)^{(q-1)/2}$, ce qui achèvera la preuve de la formule du cas pair. Nous allons en donner une preuve élémentaire, qui est une généralisation inoffensive de [H2G2, proposition VIII-3.5, figure VIII-3.1] ; pour une preuve plus sophistiquée, le lecteur est amené à

faire l'exercice A.6, qui peut être vu comme une introduction motivante à la cohomologie galoisienne.

Soit $\Omega = (-1, 0) \in W_a$. Il s'agit de l'unique point de W_a d'abscisse -1. Donc, si un point A appartient à $W_a \setminus \{\Omega\}$, la droite (ΩA), n'étant pas parallèle à la droite d'équation $X = -1$, coupe la droite Δ d'équation $X = 1$ en un unique point. Soit $f(A) = (1, 2t_A)$ ce point. Montrons que f établit une bijection entre Δ et $W_a \setminus \{\Omega\}$, si $-a$ n'est pas un carré, et que f établit une bijection entre $\Delta \setminus \{B, B'\}$ et $W_a \setminus \{\Omega\}$, si $-a$ est un carré non nul, où B et B' sont deux points distincts de Δ. Cela prouvera, dans les deux cas, grâce au symbole de Legendre, [H2G2, annexe V-C], la relation : $|W_a| = q - (-a)^{(q-1)/2}$.

On cherche donc un unique antécédent $f^{-1}(C) \in W_a \setminus \{\Omega\}$, à un point $C = (1, 2t)$ de Δ. L'équation de la droite (ΩC) est $t(1 + x) = y$ donc elle coupe W_a en un point d'abscisse x tel que $x^2 + at^2(1+x)^2 = 1$. Si $t^2 = -1/a$ (deux solutions si $-a$ est un carré, et zéro sinon), alors l'équation dégénère en une équation de degré 1 possédant pour unique solution -1, le point d'intersection étant Ω qui est interdit. Si $t \neq -1/a$, alors l'équation est du second degré et il y a une unique solution autre que -1, donc un unique $f^{-1}(C) \in W_a \setminus \{\Omega\}$, ce qui prouve l'affirmation. □

Maintenant que nous avons calculé le cardinal des nappes, le théorème est presque démontré.

Démonstration (du théorème). Le groupe $\mathrm{O}^\zeta(2n+1, \mathbb{F}_q)$ agit sur la nappe M_n^a pour $a = (-1)^n\zeta$ puisque dans ce cas la forme quadratique $Q = x_1x_2 + \cdots + x_{2n-1}x_{2n} + ax_{2n+1}^2$ a bien pour discriminant ζ. Ainsi, on peut assimiler $\mathrm{O}^\zeta(2n+1, \mathbb{F}_q)$ à $O(Q)$. Cette action est transitive par le théorème de Witt. Si $x \in M_n^a$, la droite $\langle x \rangle$ et son orthogonal $\langle x \rangle^\perp$ pour Q sont en somme directe, car x n'est pas isotrope, et le discriminant de $Q|_{\langle x \rangle^\perp}$ satisfait donc à :

$$\delta(Q|_{\langle x \rangle^\perp}) = 1 \times \delta(Q|_{\langle x \rangle^\perp}) = \delta(Q|_{\langle x \rangle})\delta(Q|_{\langle x \rangle^\perp}) = \delta(Q) = \zeta.$$

Il en résulte, par un calcul par blocs, que le stabilisateur de x dans le groupe $\mathrm{O}^\zeta(2n+1, \mathbb{F}_q)$ est isomorphe à $\mathrm{O}^\zeta(2n, \mathbb{F}_q)$. D'où l'égalité :

$$o_{2n+1}^\zeta = o_{2n}^\zeta |M_n^{(-1)^n\zeta}|.$$

De même, le groupe $\mathrm{O}^\zeta(2n, \mathbb{F}_q)$ agit sur la nappe N_n^a pour $a = (-1)^{n-1}\zeta$. Comme précédemment, cela fournit l'égalité :

$$o_{2n}^\zeta = o_{2n-1}^\zeta |N_n^{(-1)^{n-1}\zeta}|.$$

Ces deux formules produisent une récurrence pour le cas impair :

$$\begin{aligned} o^{\zeta}_{2n+1} &= o^{\zeta}_{2n-1}\left|M_n^{(-1)^n\zeta}\right| \cdot \left|N_n^{(-1)^{n-1}\zeta}\right| = \\ &= o^{\zeta}_{2n-1}q^n\Big(q^n + \big(\zeta(-1)^n\big)^{\frac{q-1}{2}}\Big)\cdot q^{n-1} \cdot \Big(q^n - \big(-\zeta(-1)^{n-1}\big)^{\frac{q-1}{2}}\Big) \\ &= o^{\zeta}_{2n-1}q^{2n-1}(q^n + \varepsilon\alpha^n)\big(q^n - \varepsilon\alpha^{n-1}\big), \end{aligned}$$

ce qui donne :

$$o^{\zeta}_{2n+1} = o^{\zeta}_{2n-1}q^{2n-1}(q^{2n} - 1).$$

Pour le cas pair, on obtient de même :

$$o^{\zeta}_{2n} = o^{\zeta}_{2n-2}q^{2n-2}(q^n - \varepsilon\alpha^n)(q^{n-1} + \varepsilon\alpha^{n-1}).$$

Il reste à regarder l'initialisation de la récurrence. On vérifie immédiatement l'égalité : $o^{\zeta}_1 = 2$. De plus, en faisant agir $\mathrm{O}^{\zeta}(2,\mathbb{F}_q)$ (transitivement) sur N^{ζ}_1, on obtient $o^{\zeta}_2 = 2(q-\varepsilon)$.

Ces deux récurrences fournissent aisément les formules du théorème. □

Et maintenant, qu'allons-nous faire de tant de bonheur ? On peut d'abord observer que le cardinal $|\mathrm{O}^{\zeta}(n,\mathbb{F}_q)|$ est donné par un polynôme dont le degré est $n(n-1)/2$. En fait, ce degré est intuitivement la dimension du groupe ; il s'agit en l'occurrence de la dimension de l'espace des matrices antisymétriques en dimension n, ce qui, en réel ou en complexe, est confirmé par le chapitre sur les algèbres de Lie. Si l'on veut regarder plus loin, le monôme de plus haut degré du polynôme est même $2q^{n(n-1)/2}$, ce qui correspond d'après le théorème de Lang-Weil[3] aux deux composantes connexes du groupe.

On peut ensuite calculer $\left|\{P\,{}^tP,\ P \in \mathrm{GL}_n(\mathbb{F}_q)\}\right|$, ce qui correspond dans le cas réel à l'ensemble $\mathscr{S}^{++}$ des produits scalaires, même si le $++$ ne signifie plus grand chose sur les corps finis. Il s'agit donc de calculer le cardinal de l'orbite de l'identité pour l'action de congruence, c'est-à-dire :

$$\left|\{P\,{}^tP,\ P \in \mathrm{GL}_n(\mathbb{F}_q)\}\right| = \left|\mathrm{GL}(\mathbb{F}_q)\right| / \left|\mathrm{O}(n,\mathbb{F}_q)\right|.$$

En faisant le calcul, on se convainc facilement qu'il s'agit d'un polynôme mais certainement pas d'un monôme. Cela signifie qu'il n'existe pas de bijection générale entre un espace vectoriel sur $\mathbb{F}_q$ et $\left|\{P\,{}^tP,\ P \in \mathrm{GL}_n(\mathbb{F}_q)\}\right|$. Autrement dit, on n'aura pas sur les corps finis l'équivalent de la bijection donnée par l'exponentielle entre l'espace de matrices symétriques et le cône des matrices symétriques définies positives.

Pour récompenser le lecteur tenace, voici une preuve simple du fait que les groupes orthogonaux de toutes les formes quadratiques non dégénérées

[3]Entre nous, quel lecteur souhaite *sincèrement* une référence ?

sont isomorphes en dimension impaire. La clé consiste à remarquer que les groupes orthogonaux de deux formes quadratiques proportionnelles sont *égaux*. Il s'agit donc de classer les formes à congruence et à scalaire près.

2.5. Corollaire. *Soit m un entier non nul et soit $\mathbb{F}_q$ un corps fini de cardinal impair.*

(i) *Si m est impair, toutes les formes quadratiques non dégénérées sont congruentes à un scalaire près et leurs groupes orthogonaux sont tous isomorphes.*

(ii) *Si m est pair, il y a deux classes de congruence de formes quadratiques à scalaire près et deux classes d'isomorphisme de groupes orthogonaux de formes quadratiques non dégénérées : elles sont déterminées par le discriminant de la forme modulo les carrés.*

Démonstration. (i) Supposons donc m impair et soit ζ un élément de $\mathbb{F}_q$ qui n'est pas un carré. La matrice diagonale $\zeta \mathrm{I}_n$ est la matrice d'une forme quadratique de discriminant ζ^m ; comme m est impair, ζ^m vaut ζ à un carré près donc ce n'est pas un carré. Ainsi, toutes les formes sont congruentes à scalaire près. Or, les groupes orthogonaux de deux formes proportionnelles sont égaux. Ainsi, il n'y a qu'une seule classe de groupes orthogonaux pour une forme non dégénérée en dimension impaire.

(ii) Supposons que m est pair. Le discriminant d'une forme Q et d'un multiple non nul λQ sont égaux à un carré près (celui de $\lambda^{m/2}$). Autrement dit, le produit par un scalaire ne fait pas sortir de la classe de congruence et il y a deux classes de congruence à scalaire près. D'après le théorème 2.1, les cardinaux des groupes orthogonaux sont différents selon le discriminant, en particuliers les groupes ne sont pas isomorphes. □

On peut calculer le cardinal des nappes $\{x \in \mathbb{F}_q^m,\ Q(x) = k\}$ $(k \in \mathbb{F}_q)$. Notons que c'est justement le calcul du cardinal des nappes qui a permis de calculer l'ordre du groupe orthogonal. On a donc le choix des méthodes pour ce calcul.

2.6. Corollaire. *Soit Q une forme quadratique non dégénérée sur $\mathbb{F}_q^m$, de discriminant ζ. Soient $\varepsilon = \zeta^{(q-1)/2} \in \{-1, 1\}$ et $\alpha = (-1)^{(q-1)/2} \in \{-1, 1\}$. Soit k dans $\mathbb{F}_q$; on note $N_k(Q)$ la nappe $\{x \in \mathbb{F}_q^m,\ Q(x) = k\}$.*

(i) *Si $m = 2n + 1$ est impair, alors on a :*

$$|N_k(Q)| = \begin{cases} q^n(q^n + \varepsilon\alpha^n) & \text{si } k \text{ est un carré non nul,} \\ q^n(q^n - \varepsilon\alpha^n) & \text{si } k \text{ n'est pas un carré,} \\ q^{2n} & \text{si } k = 0. \end{cases}$$

(ii) *Si $m = 2n$ est pair, alors on a :*

$$|N_k(Q)| = \begin{cases} q^{n-1}(q^n - \varepsilon\alpha^n) & \text{si } k \neq 0, \\ q^{2n-1} + \varepsilon\alpha^n(q^n - q^{n-1}) & \text{si } k = 0. \end{cases}$$

Démonstration. Voici une idée de preuve que le lecteur pourra compléter en exercice. On traite le cas $m = 1$ à part, et l'on remarque que, pour tout $m > 1$, les nappes $N_k(Q)$ sont non vides (on procède comme pour les nappes M_n^a et N_n^a de la preuve du théorème). On peut alors utiliser l'action de $\mathrm{O}(Q)$ sur les nappes.

Si k est non nul, le groupe orthogonal $\mathrm{O}(Q)$ agit transitivement sur la nappe par le théorème de Witt ([H2G2, corollaire V-3.5]). Le stabilisateur d'un élément x de la nappe est isomorphe à $\mathrm{O}(Q')$, où Q' est la restriction de la forme Q à l'orthogonal $\langle x\rangle^\perp$ de x. Si k est un carré non nul, alors la forme Q' est de discriminant égal au discriminant de Q. Si k n'est pas un carré, alors la forme Q' est de discriminant l'unique discriminant différent de celui de Q. Dans tous les cas, le théorème permet de calculer le cardinal de la nappe puisque $|N_k| = |\mathrm{O}(Q)|/|\mathrm{O}(Q')|$. Le cas où $k = 0$ se fait par élimination, puisque la réunion de toutes les nappes est égal à $\mathbb{F}_q^m$ et l'on sait qu'il y a $(q-1)/2$ carrés et autant de non carrés dans $\mathbb{F}_q^*$. □

3. Cardinal des grassmanniennes de sous-espaces isotropes sur un corps fini

Comme application des formules obtenues pour l'ordre des groupes orthogonaux finis, nous allons calculer des cardinaux de grassmanniennes et de variétés des drapeaux de sous-espaces totalement isotropes, dans le cadre des formes quadratiques non dégénérées sur un corps fini.

Rappels et définitions autour de l'isotropie. Soit Q une forme quadratique sur un espace E. On dit que la forme Q (ou l'espace E muni de Q) est *isotrope* s'il existe un vecteur non nul de E qui annule Q. Dans le cas contraire, on dit que la forme ou l'espace est *anisotrope*. Les *sous-espaces totalement isotropes*, que l'on abrège en *SETI*, sont les sous-espaces sur lesquels la forme Q est nulle. Comme pour l'action du groupe linéaire sur la grassmannienne, les orbites pour l'action naturelle de $\mathrm{O}(Q)$ sur l'ensemble $\mathscr{S}(Q)$ des SETI de Q sont classées par la dimension : c'est une conséquence directe du théorème de Witt, voir [H2G2, théorème V-3.4]. Tout sous-espace isotrope est contenu dans un *sous-espace totalement isotrope maximal* (*SETIM*) et tous les SETIM ont la même dimension, que l'on appelle *indice de Witt*.

3.1. Proposition. *Soit Q une forme quadratique non dégénérée sur un espace vectoriel de dimension finie m sur un corps quelconque de caractéristique différente de 2. Alors, tous les SETIM sont de même dimension $s \leqslant m/2$.*

Démonstration. Soit F un SETIM de dimension s. Comme Q est non dégénérée, on a $\dim F^\perp = m - s$. Soit φ la forme bilinéaire associée à Q ; la restriction de Q à F est nulle et la restriction de φ à $F \times F$ l'est donc également. Ainsi, $F \subset F^\perp$ et, en prenant la dimension, il vient : $s \leqslant m - s$, d'où l'inégalité.

Le fait que les dimensions de deux SETIM sont égales découle directement du théorème de Witt : supposons qu'existent deux SETIM F et F' tels que : $\dim F < \dim F'$. Alors il existe une isométrie σ de F vers un sous-espace (strict) de F' que l'on peut prolonger en une isométrie $\tilde{\sigma}$ de l'espace tout entier. Cela fait de F un SETI strictement inclus dans le SETI avéré $\tilde{\sigma}^{-1}(F')$, ce qui contredit sa maximalité. □

On notera donc dans la suite $s = s(Q)$ l'indice de Witt de la forme quadratique Q, $\mathscr{S}_r(Q)$ l'ensemble des SETI de dimension r. Enfin, on définit la variété des drapeaux isotropes :

$$\mathscr{FS}(Q) = \big\{(F_r)_{0\leqslant r\leqslant s},\ \forall r \in \{1,\dots,s\},\ F_r \in \mathscr{S}_r \text{ et } F_{r-1} \subset F_r\big\}.$$

On voit sans mal que si deux formes quadratiques Q et Q' sont congruentes, alors $\mathscr{S}_r(Q)$ et $\mathscr{S}_r(Q')$ sont en bijection, et qu'il en est de même pour $\mathscr{FS}(Q)$ et $\mathscr{FS}(Q')$ (si $Q' = Q \circ g$ avec g dans GL_n, alors g réalise cette bijection). Mieux ! Cela reste encore vrai si Q et Q' sont congruentes à un scalaire non nul près, *i.e.* si $Q' = \lambda Q \circ g$, λ non nul). Il est donc naturel, pour mener l'étude des grassmanniennes isotropes, de classer les formes quadratiques à congruence projective près. Pour les formes quadratiques non dégénérées sur le corps fini fixé $\mathbb{F}_q$, la classification nécessite un invariant déjà implicitement rencontré (sous le pseudo de $\varepsilon\alpha^n$) au moment du théorème 2.1 : on note par convention $\iota(Q) = 1$ en dimension impaire et $\iota(Q) = \zeta^{(q-1)/2}\alpha^n$ en dimension paire $m = 2n$, où ζ est le discriminant de Q et $\alpha = (-1)^{(q-1)/2}$.

Voici donc une classification des formes quadratiques sur un corps fini mieux adaptée à l'étude des SETI.

3.2. Proposition. *Soient $\mathbb{F}_q$ un corps fini de caractéristique différente de 2 et $\omega \in \mathbb{F}_q \setminus \mathbb{F}_q^2$. Soit Q une forme quadratique non dégénérée de $\mathbb{F}_q^m$. Alors, il existe une base telle que la matrice de Q soit égale, à un scalaire multiplicatif non nul près, à une et une seule des trois matrices suivantes.*

(a) *En dimension impaire* $m = 2n + 1$,

$$\mathrm{mat}(Q) = \begin{pmatrix} 0_n & \mathrm{I}_n & 0 \\ \mathrm{I}_n & 0_n & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On a dans ce cas : $s(Q) = n$ *et* $\iota(Q) = 1$.

(b) *En dimension paire* $m = 2n$,

$$\mathrm{mat}(Q) = \begin{pmatrix} 0_n & \mathrm{I}_n \\ \mathrm{I}_n & 0_n \end{pmatrix}.$$

On a dans ce cas : $s(Q) = n$ *et* $\iota(Q) = 1$.

(c) *En dimension paire* $m = 2n$,

$$\mathrm{mat}(Q) = \begin{pmatrix} 0_{n-1} & \mathrm{I}_{n-1} & 0 \\ \mathrm{I}_{n-1} & 0_{n-1} & 0 \\ 0 & 0 & W \end{pmatrix}, \quad \textit{avec } W = \begin{pmatrix} 1 & 0 \\ 0 & -\omega \end{pmatrix}.$$

On a dans ce cas : $s(Q) = n - 1$ *et* $\iota(Q) = -1$.

Démonstration. On fixe une base $(e_1, \ldots, e_m)$ de l'espace. Montrons tout d'abord que l'on a bien ces trois cas.

On a vu dans le corollaire 2.5 qu'en dimension impaire, toutes les formes quadratiques non dégénérées sont congruentes à scalaire près. Il suffit donc de vérifier que le déterminant de la matrice du cas (a) n'est pas nul, ce qui résulte par exemple d'un développement par blocs.

Dans le cas pair, on a deux classes de congruence à scalaire près. On vérifie que dans le cas (b), le déterminant est $(-1)^n$ et dans le cas (c), c'est $(-1)^n\omega$. On recouvre donc bien les deux possibilités pour le discriminant.

Calculons $\iota(Q)$. Dans le cas impair, c'est 1 par définition. Dans le cas pair, on a $\iota(Q) = \big((-1)^n \det(Q)\big)^{(q-1)/2}$ qui vaut 1 dans le cas (b) et $\omega^{(q-1)/2}$ dans le cas (c). Comme ω n'est pas un carré, ce dernier nombre vaut -1.

Calculons enfin les indices de Witt. On remarque à l'oeil nu que pour une forme quadratique dont la matrice est $\left(\begin{smallmatrix} 0_n & \mathrm{I}_n \\ \mathrm{I}_n & 0_n \end{smallmatrix}\right)$, les n premiers vecteurs de la base engendrent un SETI de dimension n.

(a) On sait que $s \leqslant m/2$, donc $s \leqslant n$. D'après la remarque précédente, il existe un SETI de dimension n, il est donc maximal et l'on a : $\iota(Q) = n$.

(b) On a un SETI de dimension n et la relation : $s \leqslant m/2 = n$, d'où le résultat.

(c) On a un SETI F de dimension $n - 1$ et la relation : $s \leqslant m/2 = n$. Il reste à montrer qu'il n'existe pas de sous-espace totalement isotrope de dimension n. Supposons qu'il en existe un. Alors, par transitivité du groupe orthogonal (proposition 3.1), F est inclus dans un

SETIM F' de dimension n. Par la formule de Grassmann, l'intersection $F' \cap \langle e_n, \dots, e_{2n-2}, e_{2n-1}, e_{2n}\rangle$ est de dimension supérieure à 1, donc contient au moins un élément non nul f. On décompose f selon la somme directe $\langle e_n, \dots, e_{2n-2}\rangle \oplus \langle e_{2n-1}, e_n\rangle$, soit : $f = u + w$. On a par hypothèse : $0 = q(f) = q(u) + q(w) = q(w)$, d'où : $w = 0$, puisque W est anisotrope (c'est une conséquence immédiate du fait que ω n'est pas un carré). Donc f possède une coordonnée non nulle, disons en e_j, avec $n \leqslant j \leqslant 2n-2$, qui est d'autre part égale à $\varphi(e_{j-n}, f)$ (rappel : φ est la forme polaire de Q). Or, e_{j-n} appartient à $F \subset F'$ et Q s'annule sur F', d'où : $\varphi(e_{j-n}, f) = 0$. Absurbe. □

En vertu de cette proposition, il sera pratique de noter Q^{ι}_m une forme quadratique Q en dimension m et telle que $\iota(Q) = \iota$. D'après la classification obtenue dans la proposition et les remarques qui la précèdent, il reste maintenant à calculer les cardinaux de grassmanniennes et de variétés des drapeaux de sous-espaces totalement isotropes pour Q^{ι}_m pour m impair, $\iota = 1$ et pour m pair, $\iota = \pm 1$. On peut récrire le théorème 2.1 de la façon suivante :

$$\left|\mathrm{O}(Q^{\iota}_{2n+1})\right| = 2q^n \prod_{k=0}^{n-1}(q^{2n} - q^{2k}), \quad \left|\mathrm{O}(Q^{\iota}_{2n})\right| = 2(q^n - \iota)\prod_{k=1}^{n-1}(q^{2n} - q^{2k}).$$

Selon une méthode inextirpable du présent ouvrage, nous allons dans chaque cas faire agir ces groupes de façon transitive sur les ensembles étudiés et considérer certains stabilisateurs.

3.3. Lemme. *Soit W une matrice symétrique associée à une forme quadratique Q_W anisotrope sur $\mathbb{F}_q^d$. Soient M et S deux matrices données par la même structure par blocs :*

$$M = \begin{pmatrix} A & B & C \\ 0 & D & E \\ F & G & H \end{pmatrix}, \quad S = \begin{pmatrix} 0_s & \mathrm{I}_s & 0_{s,d} \\ \mathrm{I}_s & 0_s & 0_{s,d} \\ 0_{d,s} & 0_{d,s} & W \end{pmatrix}.$$

Alors, M stabilise S par congruence si et seulement si les équations suivantes sont satisfaites :

$$A\,{}^tD = \mathrm{I}_s,\ B\,{}^tA + A\,{}^tB + CW\,{}^tC = 0_s,\ A\,{}^tG + CW\,{}^tW = 0_{s,d},$$
$$E = 0_{s,d},\ F = 0_{d,s},\ HW\,{}^tH = W.$$

3.4. Remarque. On note que l'ensemble des solutions de ce système peut être paramétré par A dans $\mathrm{GL}_s(\mathbb{F}_q)$, C dans $\mathscr{M}_{s,d}(\mathbb{F}_q)$, H dans $\mathrm{O}(Q_W)$ et, enfin, B dans un espace affine de dimension $s(s-1)/2$. En effet, l'équation $B\,{}^tA + A\,{}^tB = K$, si K est symétrique, est celle d'un espace affine, non vide

puisque $K\,{}^tA^{-1}/2$ est solution, et son espace vectoriel associé, d'équation $B\,{}^tA + A\,{}^tB = 0_s$ est isomorphe à l'espace des matrices antisymétriques via l'isomorphisme $B \mapsto B\,{}^tA^{-1}$.

Démonstration. En écrivant par blocs l'égalité $MS\,{}^tM = S$, on obtient les équations suivantes :

$$\begin{aligned} A\,{}^tD + CW\,{}^tE &= \mathrm{I}_s, & B\,{}^tA + A\,{}^tB + CW\,{}^tC &= 0_s, \\ B\,{}^tFA\,{}^tG + CW\,{}^tW &= 0_{s,d}, & EW\,{}^tE &= 0_s, \\ D\,{}^tF + EW\,{}^tH &= 0_{s,d}, & G\,{}^tF + F\,{}^tG + HW\,{}^tH &= W. \end{aligned}$$

L'équation $EW\,{}^tE = 0_s$ dit que l'image de ${}^tE$ est dans un sous-espace isotrope pour Q_W. Or, Q_W est par hypothèse anisotrope, donc ${}^tE$ est nulle. Ainsi, E est la matrice nulle. On en tire : $A\,{}^tD = \mathrm{I}_s$, et donc F est nulle, car D est inversible. Les autres équations viennent alors sans difficulté. □

Pour une forme quadratique Q sur un corps fini, on va noter $S(Q)$ le cardinal de l'ensemble de ses SETIM (de dimension s), $S_r(Q)$ le cardinal de l'ensemble de ses SETI de dimension r et $\mathscr{F}(Q)$ le cardinal de l'ensemble de ses drapeaux complets de sous-espaces isotropes.

Voici donc la solution au problème de dénombrement des grassmanniennes isotropes et variétés des drapeaux de sous-espaces isotropes.

3.5. Proposition. *Soit $Q = Q_m^\iota$ une forme quadratique en dimension m, avec $\iota(Q) = 1$ pour m impair et $\iota(Q) = \zeta^{(q-1)/2}\alpha^n$ pour $m = 2n$, où ζ est le discriminant de Q_m^ι et $\alpha = (-1)^{(q-1)/2}$. Le cardinal de l'ensemble des SETIM, le cardinal de l'ensemble des SETI de dimension r, et le cardinal des drapeaux complets de SETI, sont donnés ainsi.*

(a) *Si $m = 2n+1$, alors :*

$$S(Q_m^\iota) = \prod_{k=1}^{n}(q^k+1), \qquad S_r(Q_m^\iota) = \begin{bmatrix} n \\ r \end{bmatrix}_q \prod_{k=n-r+1}^{n}(q^k+1),$$

$$\mathscr{F}(Q_m^\iota) = \prod_{k=1}^{n}[2k]_q.$$

(b) *Si $m = 2n$ et $\iota = 1$, alors :*

$$S(Q_m^\iota) = \prod_{k=0}^{n-1}(q^k+1), \qquad S_r(Q_m^\iota) = \begin{bmatrix} n \\ r \end{bmatrix}_q \prod_{k=n-r}^{n-1}(q^k+1),$$

$$\mathscr{F}(Q_m^\iota) = 2[n]_q \prod_{k=1}^{n-1}[2k]_q.$$

(c) *Si* $m = 2n$ *et* $\iota = -1$, *alors :*

$$S(Q_m^\iota) = \prod_{k=2}^{n}(q^k+1), \qquad S_r(Q_m^\iota) = \begin{bmatrix} n-1 \\ r \end{bmatrix}_q \prod_{k=n-r+1}^{n}(q^k+1),$$

$$\mathscr{F}(Q_m^\iota) = (q^n+1)\prod_{k=2}^{n-1}[2k]_q.$$

3.6. Remarque. Pour $r = 1$, on retrouve le corollaire 2.6 dans le cas $k = 0$.

Démonstration. Les formules pour les cardinaux $S(Q_m^\iota)$ et $\mathscr{F}(Q_m^\iota)$ proviennent du théorème de Witt, qui assure une action transitive sur l'ensemble des SETIM et sur l'ensemble des drapeaux complets de sous-espaces isotropes. Pour le premier, on est amené à chercher le stabilisateur $\mathrm{O}(Q_m^\iota)_F$ du SETIM $F = \langle e_1, \dots, e_s\rangle$; pour le second, le stabilisateur $\mathrm{O}(Q_m^\iota)_{\mathscr{F}}$ du drapeau $\mathscr{F} = \langle e_1\rangle \subset \langle e_1, e_2\rangle \subset \cdots \subset \langle e_1, \dots, e_s\rangle$. D'après le lemme 3.3 et la remarque qui suit, ces stabilisateurs ont pour cardinaux :

$$\big|\mathrm{O}(Q_m^\iota)_F\big| = \big|\mathrm{GL}_s(\mathbb{F}_q)\big|\, q^{\frac{s(s-1)}{2}}\, q^{ds}\big|\mathrm{O}(Q_W)\big|,$$

$$\big|\mathrm{O}(Q_m^\iota)_{\mathscr{F}}\big| = \big|B_s(\mathbb{F}_q)\big|\, q^{\frac{s(s-1)}{2}}\, q^{ds}\big|\mathrm{O}(Q_W)\big|,$$

où $B_s(\mathbb{F}_q)$ est le sous-groupe des matrices triangulaires supérieures de $\mathrm{GL}_s(\mathbb{F}_q)$. Notons que Q_W est une forme quadratique anisotrope de degré d, où d vaut 1, 0, ou 2 selon que l'on est respectivement dans les cas (a), (b) ou (c). Dans le cas où $d = 0$, le groupe $\mathrm{O}(Q_W)$ est trivial ; pour $d = 1$, c'est $\{\pm 1\}$; pour $d = 2$, le fait que Q_W soit anisotrope et le théorème 2.1 entraînent que $\mathrm{O}(Q_W)$ est un groupe[4] d'ordre $q+1$.

Les formules s'obtiennent sans mal à partir des égalités

$$S(Q_m^\iota) = \frac{\big|\mathrm{O}(Q_m^\iota)\big|}{\big|\mathrm{O}(Q_m^\iota)_F\big|}, \quad \mathscr{F}(Q_m^\iota) = \frac{\big|\mathrm{O}(Q_m^\iota)\big|}{\big|\mathrm{O}(Q_m^\iota)_{\mathscr{F}}\big|}.$$

Il reste à trouver le nombre de SETI de dimension r. Il est naturel de passer, selon une technique éprouvée[5] de « tiré en arrière-poussé en avant », par l'ensemble intermédiaire

$$\big\{(F, F'),\ F \subset F' \text{ isotropes},\ \dim F = r,\ \dim F' = s\big\}.$$

Le cardinal de cet ensemble est égal (par le lemme du berger, donc !) au nombre de SETIM F' multiplié par le nombre de sous-espaces de dimension r de F' (qui ne dépend pas de F'). Ce cardinal est donc $\begin{bmatrix} s \\ r \end{bmatrix}_q S(Q_m^\iota)$.

[4] Au passage, c'est un groupe cyclique, comme dans [H2G2, proposition VIII-3.5].

[5] C'est la même méthode que pour le calcul du cardinal du cône isotrope sur un corps fini, voir la partie 4. Même si ici, elle est réduite à son expression la plus élémentaire, en l'occurrence le célèbre lemme du berger, il est remarquable d'en retrouver des avatars aux niveaux les plus vertigineux de la géométrie algébrique.

Montrons que, pour la forme quadratique Q_m^ι, le nombre de SETIM contenant un SETI F fixé de dimension r est égal à $S(Q_{m-2r}^\iota)$ (et ne dépend donc pas du SETI F choisi). On aura ainsi

$$S_r(Q_m^\iota) = \frac{\begin{bmatrix} s \\ r \end{bmatrix}_q S(Q_m^\iota)}{S(Q_{m-2r}^\iota)},$$

ce qui donnera sans embûche les formules de la proposition.

Soit donc F un SETI de dimension r pour la forme quadratique Q_m^ι. Le sous-espace $F^\perp$ contient F puisque F est totalement isotrope. L'assertion que nous voulons prouver résultera alors des deux assertions suivantes.

1. La forme quadratique $Q_m^\iota|_{F^\perp}$ passe au quotient en une forme quadratique de $F^\perp/F$ et la forme $\bar{Q}_m^\iota$ ainsi obtenue est congruente à Q_{m-2r}^ι.
2. Le passage au quotient par F fournit une bijection entre les SETIM de Q_m^ι qui contiennent F et les SETIM de $\bar{Q}_m^\iota$.

Montrons le premier point. Quitte à utiliser l'action de $\mathrm{O}(Q_m^\iota)$ et le théorème de Witt, on peut se ramener au cas où $F = \langle e_1, e_2, \ldots, e_r \rangle$. Dans ce cas, on a la décomposition :

$$F^\perp/F = \langle \bar{e}_{r+1}, \ldots, \bar{e}_s \rangle \oplus \langle \bar{e}_{s+r+1}, \ldots, \bar{e}_{2s} \rangle \oplus \langle \bar{e}_{m-d+1}, \bar{e}_m \rangle.$$

La forme quadratique Q_m^ι passe au quotient puisque l'on travaille modulo F, qui est *a priori* dans le noyau de $Q|_{F^\perp}$ (et *a posteriori* égal au noyau). Dans la base $(\bar{e}_{r+1}, \ldots, \bar{e}_s, \bar{e}_{s+r+1}, \ldots, \bar{e}_{2s}, \bar{e}_{m-d+1}, \bar{e}_m)$, on reconnaît alors la matrice de la forme quadratique non dégénérée Q_{m-2r}^ι.

Montrons le second point. Tout d'abord, si F' est un SETIM de Q_m^ι contenant F, alors on a : $F' \subset F'^\perp \subset F^\perp$. Parallèlement, on sait que le quotient par F fournit une bijection entre les sous-espaces de dimension s de $F^\perp$ contenant F et les sous-espaces de dimension $s-r$ de $F^\perp/F$. Par construction de la forme quadratique sur $F^\perp/F$, cette bijection envoie les sous-espaces isotropes de dimension s de $F^\perp$ vers les sous-espaces isotropes de dimension $s-r$. Mais les sous-espaces isotropes de dimension s de $F^\perp$ sont des SETIM de Q_m^ι et les sous-espaces isotropes de dimension $s-r$ sont les SETIM de $\bar{Q}_m^\iota$, d'après le premier point. □

3.7. Remarque. On devine que ces formules de cardinaux sont les ombres de décompositions naturelles en cellules de grassmanniennes de sous-espaces isotropes sur $\mathbb{F}_q$. Y a-t-il un équivalent de la décomposition en cellules de la grassmannienne classique ? Valable sur $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{F}_q$? Le doute est permis, puisque la classification des formes quadratiques change du tout au tout selon le corps de base.

4. Cardinal du cône nilpotent sur un corps fini

Le cône nilpotent $\mathcal{N}_d = \mathcal{N}_d(\mathbb{K})$, constitué des matrices $d \times d$ nilpotentes sur un corps $\mathbb{K}$ est un objet convoité dans plusieurs domaines des mathématiques. On le rencontre en géométrie algébrique, théorie de Lie, théorie des représentations...

Estimons heuristiquement le cardinal de $\mathcal{N}_d$ sur un corps fini. Sur les complexes, l'orbite du bloc de Jordan J_d est ouverte et dense dans $\mathcal{N}_d$. En étant optimiste, on extrapole sur un corps fini de cardinal q : « presque tous » les éléments de $\mathcal{N}_d$ sont dans l'orbite $\mathcal{O}_{J_d}$ de J_d. Or, on peut identifier $\mathcal{O}_{J_d}$ au quotient de GL_d par le stabilisateur de J_d, c'est-à-dire le commutant de J_d dans GL_d, qui est le sous-groupe constitué des polynômes en J_d. Le groupe linéaire (resp. le commutant de J_d) a pour cardinal q^{d^2} (resp. q^d) donc le cardinal de $\mathcal{N}_d$ doit être équivalent (pour q grand) à q^{d^2-d}.

Surprise : c'est *exactement* q^{d^2-d}. Voici une explication — toujours heuristique mais bien plus savante. Une des particularités de $\mathcal{N}_d$ est d'être une variété algébrique[6] possédant des invariants topologiques semblables à ceux d'un espace affine mais des invariants algébriques distincts de celui-ci. Les gens familiers des *conjectures de Weil* ne seront pas surpris que le cardinal du cône nilpotent sur le corps fini $\mathbb{F}_q$ soit celui d'un espace affine.

En revanche, les preuves élémentaires de ce résultat ne sont pas légion. L'idée la plus naturelle calculer le cardinal de $\mathcal{N}_d$ est de décomposer $\mathcal{N}_d$ en orbites pour l'action de conjugaison de GL_d et de sommer sur les classes de similitude, c'est-à-dire sur les diagrammes de Young. Mais le calcul des stabilisateurs (utile pour dénombrer les orbites) est fastidieux, et la somme ne laisse pas simplifier facilement. La méthode qui suit est inspirée de ce que l'on appelle la *désingularisation de Springer*. Comme le disait naguère Marc Miroil : « c'est une méthode qui torche ! ». Traduire : elle nettoie efficacement un problème délicat.

Pour tout corps $\mathbb{K}$, on note $\mathcal{N}_d(\mathbb{K})$ le cône des matrices nilpotentes de taille $d \times d$ sur le corps $\mathbb{K}$. Le but de cette est donc de montrer le théorème suivant.

4.1. Théorème. *Pour tout corps fini $\mathbb{F}_q$ de cardinal q et tout entier d, on a :*

$$\left|\mathcal{N}_d(\mathbb{F}_q)\right| = q^{d(d-1)}.$$

On fixe un espace vectoriel E de dimension d et l'on identifie $\mathcal{N}_d = \mathcal{N}_d(\mathbb{F}_q)$ aux endomorphismes nilpotents de E. Commençons par montrer la proposition suivante.

[6] Comme ensemble, c'est le lieu des zéros communs d'une famille de polynômes, les coefficients du polynôme caractéristique.

4.2. Proposition. *Soient $N \in \mathcal{N}_d$ et e un vecteur non nul dans E. On note r le nombre maximal tel que $\mathbf{e} = (e, Ne, N^2e, \dots, N^{r-1}e)$ est une famille libre. On a alors : $N^r e = 0$.*

Démonstration. Soit F le sous-espace de E engendré par e et N, c'est-à-dire : $F = \langle N^s e,\ s \in \mathbb{N} \rangle$. Alors, on peut affirmer que $\mathbf{e}$ est une base de F. En effet, elle est libre par construction. Montrons qu'elle est génératrice : pour cela, il suffit de voir que pour tout $s \geqslant r$, on a $N^s e \in F$. Pour $s = r$, c'est encore vrai puisque par construction, on peut écrire $N^r e = \sum_{i=0}^{r} a_i N^i e$ pour des scalaires $a_0, \dots, a_{r-1}$ convenables. C'est enfin vrai par récurrence pour tout $s \geqslant r$, car $N^s e = \sum_{i=0}^{d} a_i N^{s-r+i} e$.

Par construction, N stabilise F, on note $N' = N_F$ l'endomorphisme induit par la restriction de N à F. Sa matrice dans la base $\mathbf{e}$ est donc

$$\begin{pmatrix} 0 & \cdots & 0 & a_0 \\ 1 & & \vdots & \vdots \\ 0 & \ddots & 0 & \vdots \\ 0 & 0 & 1 & a_{r-1} \end{pmatrix}.$$

On reconnaît alors la *matrice compagnon* du polynôme $P = X^r - \sum_{i=0}^{d} a_i X^i$, dont le polynôme caractéristique est justement le polynôme P (qui est également minimal). Comme N' est nilpotente, tous les a_i valent 0, ce qui termine la preuve de la proposition. □

Prouvons maintenant le théorème. Soit $L_{r,d}$ l'ensemble des parties libres dans E à r éléments. On dit que N *respecte* une famille $\mathbf{e} = (e_1, \dots, e_r)$ de $L_{r,d}$ si, pour tout s entier entre 1 et r, on a : $Ne_s = e_{s+1}$ —on convient que e_{r+1} est nul.

Posons maintenant $n_d = |\mathcal{N}_d|$ et déterminons une formule de récurrence pour n_d. Pour cela, calculons de deux manières le cardinal de l'ensemble

$$\tilde{\mathcal{N}_d} = \big\{(N, \mathbf{e}),\ N \in \mathcal{N}_d, \exists r \in \{1, \dots, d\},\ \mathbf{e} \in L_{r,d} \text{ et } N \text{ respecte } \mathbf{e}\big\}.$$

On note π_1 (resp. π_2), la projection sur la première (resp. seconde) composante.

Premier calcul. Un élément de $\pi_1^{-1}(N)$ est entièrement déterminé par un vecteur non nul e_1 de E, puisqu'il s'écrira alors $\big(N, (e_1, Ne_1, \dots, N^{r-1}e_1)\big)$ pour r convenable. On en déduit donc : $|\pi_1^{-1}(N)| = q^d - 1$, puis[7] :

$$|\tilde{\mathcal{N}_d}| = \sum_{N \in \mathcal{N}_d} |\pi_1^{-1}(N)| = n_d(q^d - 1).$$

[7] Mais pourquoi tant de N ?

Deuxième calcul. On a :

$$|\tilde{\mathcal{N}_d}| = \sum_{r=1}^{d} \sum_{\mathbf{e} \in L_{r,d}} |\pi_2^{-1}(\mathbf{e})|.$$

Fixons r entre 1 et d et notons g_r l'ordre du groupe $\mathrm{GL}(k^r)$. L'action naturelle de $\mathrm{GL}(E)$ sur $L_{r,d}$ est transitive d'après le théorème de la base incomplète. Fixons $\mathbf{e}$ dans $L_{r,d}$ et complétons-la en une base $\tilde{\mathbf{e}}$ de E. Dans cette base, le stabilisateur de $\mathbf{e}$ s'écrit sous la forme : $\left(\begin{smallmatrix} \mathrm{I}_r & M \\ 0 & B \end{smallmatrix}\right)$, avec M dans $\mathscr{M}_{r,d-r}(\mathbb{F}_q)$, $B \in \mathrm{GL}_{d-r}(\mathbb{F}_q)$. Il vient donc :

$$|L_{r,d}| = \frac{g_d}{g_{d-r} q^{r(d-r)}}.$$

Maintenant, une matrice nilpotente N respecte $\mathbf{e}$ si et seulement si la matrice de l'application linéaire associée à N dans une base $\tilde{\mathbf{e}}$ est de la forme :

$$\mathrm{mat}_{\tilde{\mathbf{e}}} = \begin{pmatrix} J_r & M \\ 0 & N_{d-r} \end{pmatrix},$$

où M est une matrice quelconque de $\mathscr{M}_{r,d-r}$, N_{d-r} une matrice nilpotente de taille $(d-r) \times (d-r)$ et J_r est le bloc de Jordan de taille $r \times r$. On obtient alors :

$$|\tilde{\mathcal{N}_d}| = \sum_{r=1}^{d} |L_{r,d}| q^{r(d-r)} n_{d-r} = \sum_{r=1}^{d} \frac{g_d}{g_{d-r}} n_{d-r}.$$

En comparant les deux calculs, on obtient la formule de récurrence :

$$\frac{n_d}{g_d} = \frac{1}{q^d - 1} \sum_{r=1}^{d} \frac{n_{d-r}}{g_{d-r}}.$$

Pour r compris entre 1 et d, notons $m_r = n_r / g_r$. Il vient :

$$(q^d - 1) m_d = \sum_{r=0}^{d-1} m_r = m_{d-1} + \sum_{r=0}^{d-2} m_r = m_{d-1} + (q^{d-1} - 1) m_{d-1} = q^{d-1} m_{d-1}.$$

On en tire aisément la relation :

$$m_d = \frac{q^{d(d-1)/2}}{\prod_{r=1}^{d} (q^r - 1)} = \frac{q^{d(d-1)}}{g_d},$$

et finalement : $n_d = q^{d(d-1)}$.

On trouve dans l'exercice A.5 une autre preuve de ce résultat, qui nous a été signalée par Pierre Baumann et qui utilise le fameux *lemme de Fitting.*

A. Exercices du chapitre IV

Dans tous les exercices, q est une puissance d'un nombre premier impair.

Matrices et rang

Dans les trois exercices suivants, on fixe trois entiers m, n et r tels que $0 \leqslant r \leqslant \min(m,n)$.

A.1. Exercice (Nombre de matrices dont l'image est fixée)

Soit F un sous-espace de $\mathbb{F}_q^m$ de dimension r. On veut calculer le cardinal de l'ensemble I_F des matrices de $\mathscr{M}_{m,n}(\mathbb{F}_q)$ dont l'image est F.

1. *Montrer que I_F est une orbite pour l'action par multiplication à droite de $\mathrm{GL}_n(\mathbb{F}_q)$ sur $\mathscr{M}_{m,n}(\mathbb{F}_q)$.*
   C'est en fait dans [H2G2, théorème IV-2.5].
2. *Montrer que le cardinal ne dépend que de r et pas du sous-espace F.*
   Pour F et F' deux tels sous-espaces, choisir une matrice de $\mathrm{GL}_m(\mathbb{F}_q)$ qui envoie l'un sur l'autre et en déduire une bijection de I_F sur $I_{F'}$.
3. *On suppose dans la suite que F est le sous-espace engendré par les r premiers vecteurs de la base canonique de $\mathbb{F}_q^m$. Calculer le stabilisateur de la matrice $\left(\begin{smallmatrix} \mathrm{I}_r & 0 \\ 0 & 0 \end{smallmatrix}\right) \in \mathscr{M}_{m,n}(\mathbb{F}_q)$ pour l'action par multiplication à droite de $\mathrm{GL}_n(\mathbb{F}_q)$.*
4. *En déduire que le cardinal cherché est donné par :*

$$q^{\frac{r(r-1)}{2}} \prod_{k=n-r+1}^{n} (q^k - 1).$$

A.2. Exercice (Nombre de matrices dont le noyau est fixé)

On veut calculer le cardinal de l'ensemble I_K des matrices de $\mathscr{M}_{m,n}(\mathbb{F}_q)$ dont le noyau est un sous-espace de $\mathbb{F}_q^n$ fixé K de dimension r. En utilisant la dualité et l'exercice A.1, montrer que le cardinal cherché est donné par :

$$q^{\frac{(n-r)(n-r-1)}{2}} \prod_{k=r+1}^{n} (q^k - 1).$$

A.3. Exercice (Nombre de matrices dont l'image *et* le noyau sont fixés)

On veut calculer le cardinal de l'ensemble $I_{F,K}$ des matrices de $\mathscr{M}_{m,n}(\mathbb{F}_q)$ dont l'image est un sous-espace de $\mathbb{F}_q^m$ fixé F de dimension r et le noyau, un sous-espace fixé K de dimension $n-r$ (forcément !).

1. *Montrer que le cardinal ne dépend pas du sous-espace F de dimension r ni du sous-espace K de dimension $n-r$.*
2. *En supposant dans la suite que F est le sous-espace engendré par les r premiers vecteurs de la base canonique de $\mathbb{F}_q^m$ et que K est le sous-espace engendré par les $n-r$ derniers vecteurs de la base canonique de $\mathbb{F}_q^n$, montrer que le cardinal cherché est égal à $|\mathrm{GL}_r(\mathbb{F}_q)|$.*

A.4. Exercice (Nombre de matrices de rang fixé)

Montrer à l'aide des exercices qui précèdent que le nombre de matrices de $\mathscr{M}_{m,n}(\mathbb{F}_q)$ de rang r est égal à $\big|\mathrm{GL}_r(\mathbb{F}_q)\big|\,\big|\mathrm{Gr}_{r,m}(\mathbb{F}_q)\big|\,\big|\mathrm{Gr}_{n-r,n}(\mathbb{F}_q)\big|$. Puis réinterpréter les résultats des exercices A.1 et A.2 en termes de cardinaux.

Cône nilpotent

A.5. Exercice (Cardinal du cône nilpotent)

1. Lemme de Fitting *: soit u un endomorphisme d'un espace vectoriel E de dimension finie. Montrer que la suite croissante des sous-espaces vectoriels $\big(\ker(u^k)\big)_{k\geqslant 0}$ et la suite décroissante des sous-espaces vectoriels $\big(\mathrm{im}(u^k)\big)_{k\geqslant 0}$ stationnent à partir d'un certain rang n_0 et que l'on a : $E = \ker(u^{n_0}) \oplus \mathrm{im}(u^{n_0})$. Montrer que l'endomorphisme $u_{\ker(u^{n_0})}$ est nilpotent et que $u_{\mathrm{im}(u^{n_0})}$ est un isomorphisme.*

   Cela ne devrait pas être nécessaire mais tout est fait dans la proposition III-A.9.

2. *Soit $m_{k,d}$ le nombre de couples de sous-espaces (F,G) de $\mathbb{F}_q^d$ tels que $\dim F = k$ et $F \oplus G = \mathbb{F}_q^d$. En utilisant une action transitive de $\mathrm{GL}_d(\mathbb{F}_q)$, montrer que l'on a :*

$$m_{k,d} = \frac{\big|\mathrm{GL}_d(\mathbb{F}_q)\big|}{\big|\mathrm{GL}_k(\mathbb{F}_q)\big|\,\big|\mathrm{GL}_{d-k}(\mathbb{F}_q)\big|}.$$

3. *Soit n_d le nombre de matrices nilpotentes de taille $d \times d$ à coefficients dans $\mathbb{F}_q$. Montrer l'égalité :*

$$\sum_{k=0}^{d} m_{k,d} n_k \big|\mathrm{GL}_{d-k}(\mathbb{F}_q)\big| = q^{d^2}.$$

   On pourra chercher une réciproque à la question 1 en montrant que tout endomorphisme u peut être construit à partir de deux sous-espaces supplémentaires F et G stables par u tels que u_F est nilpotent et u_G est un isomorphisme.

4. *En comparant cette formule avec celle obtenue en remplaçant d par $d-1$, montrer que $n_d = q^{d(d-1)}$.*

5. *On note maintenant $n_{r,d}$ le nombre de matrices nilpotentes de rang r et $o_{r,d}$ le nombre de matrices de rang r (de taille d), calculé dans l'exercice A.4. Montrer comme dans la question 3 la relation :*

$$\sum_{k=d-r}^{d} m_{k,d}\left|\mathrm{GL}_{d-k}(\mathbb{F}_q)\right| n_{r-d+k,k} = o_{r,d}.$$

6. *En comparant cette formule avec celle obtenue en remplaçant d par $d-1$ et r par $r-1$, montrer l'égalité :*

$$n_{r,d} = \begin{bmatrix} d \\ r \end{bmatrix}_q \begin{bmatrix} d-1 \\ r \end{bmatrix}_q \left|\mathrm{GL}_r(\mathbb{F}_q)\right|.$$

Formes quadratiques et formes symplectiques sur un corps fini

A.6. Exercice (Paramétrage du cercle et cohomologie galoisienne)
Soit $a \in \mathbb{F}_q$, soit Q la forme quadratique $Q(X,Y) = X^2 + aY^2$, sur $\mathbb{F}_q^2$, et soit W_a la nappe $\{(X,Y),\ Q(X,Y) = 1\}$. Nous voulons montrer la relation : $|W_a| = q - (-a)^{(q-1)/2}$.

1. *On suppose $(-a)^{(q-1)/2} = 1$. Montrer que Q a pour matrice, dans une base convenable, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. En déduire que l'on a : $|W_a| = q-1$.*
Le discriminant de Q est égal à a et le discriminant de $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ est -1. Par hypothèse, $-a$ est un carré donc que les discriminants sont égaux. Le cardinal de W_a est alors égal au cardinal de $\{(x,y),\ 2xy = 1\}$.
2. *On suppose $(-a)^{(q-1)/2} = -1$. Soit donc $\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, tel que $\omega^2 = -a$, de sorte que l'on a : $W_a = \{(X,Y) \in \mathbb{F}_q^2,\ (X+\omega Y)(X-\omega Y) = 1\}$. Soit $\sigma : z \mapsto z^q$ l'automorphisme de Frobenius de $\mathbb{F}_{q^2}$, soient $N : \mathbb{F}_{q^2} \to \mathbb{F}_q$, $z \mapsto z\sigma(z) = z^{q+1}$ sa norme et $\phi : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$, $z \mapsto z^{q-1}$.*
Montrer que l'on a la suite exacte de groupes :

$$1 \longrightarrow \mathbb{F}_q^* \xrightarrow{\ \iota\ } \mathbb{F}_{q^2}^* \xrightarrow{\ \phi\ } \mathbb{F}_{q^2}^* \xrightarrow{\ N\ } \mathbb{F}_q^* \longrightarrow 1,$$

où ι est l'injection naturelle.
Comme on a : $z^{q^2-1} = 1$ pour tout z de $\mathbb{F}_{q^2}^*$, il vient : $\mathrm{im}(\phi) \subset \ker(N)$. Or, on a aussi : $|\mathrm{im}(\phi)| = |\mathbb{F}_{q^2}^*| / \ker(\phi)| = q+1$ et $|\ker(N)| \leqslant q+1$, car c'est le nombre de racines d'un polynôme de degré $q+1$ sur un corps.
3. *On suppose toujours $(-a)^{(q-1)/2} = -1$. Conclure : $|W_a| = q+1$.*
On a $\sigma(\omega) = -\omega$ car c'est l'autre racine de l'équation $z^2 = -a$, de sorte que l'on a : $\sigma(x+\omega y) = x - \omega y$ pour tous x, y de $\mathbb{F}_q$. Montrer par un changement de variable approprié que l'on a l'égalité : $W_a = \{(X,Y),\ N(X+\omega Y) = 1\}$...

Nous avons ici un peu plus qu'un cardinal. Nous avons montré que lorsque -1 n'est pas un carré, alors $x^2+y^2=1$ peut se paramétrer par $(x,y)=\phi(z)$. Remarquons que $\phi(z)$ est le quotient de l'image de z par l'automorphisme non trivial du groupe de Galois de $\mathbb{F}_{q^2}/\mathbb{F}_q$ par z.
La même suite exacte, adaptée au corps $\mathbb{Q}$, donne la paramétrisation algébrique bien connue du cercle via les formules de la tangente de l'arc-moitié : si $x+iy$ est de norme 1 dans $\mathbb{Q}(i)$, il existe $z_0=x_0-iy_0\in\mathbb{Q}(i)$ tel que

$$x+iy=\frac{\bar{z}_0}{z_0}=\frac{1-t^2}{1+t^2}+i\frac{2t}{1+t^2},$$

avec $t=y_0/x_0$. On constate alors que celles-ci proviennent du fait qu'un noyau — un ker — (équation implicite) est une image — un im — (équation paramétrique).
La possibilité de passer du ker à l'im provient souvent de l'annulation d'un groupe de cohomologie. Ici, il s'agit du groupe de cohomologie galoisienne $H^1\big(\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q),\mathbb{F}_{q^2}^*\big)$. C'est une façon sophistiquée d'exprimer par une annulation de cohomologie, le célèbre *théorème 90 de Hilbert*, et les formules de l'arc-moitié.

A.7. Exercice. *Soit m un entier, soit Q une forme quadratique non dégénérée sur $\mathbb{F}_q^m$ de matrice S dans la base canonique et soit r un entier tel que $0\leqslant r\leqslant m$. Calculer, dans les trois cas de la proposition 3.5, le nombre de matrices P de $\mathscr{M}_{m,r}$ telles que ${}^tPSP$ est nulle.*

On montrera que cela revient à dire que $\mathrm{im}(P)$ est totalement isotrope pour Q. On classera les matrices P selon leur image (qui est un SETI) et lorsque l'image est fixée, on pourra utiliser l'exercice A.1.

A.8. Exercice (Nombre de lagrangiens)

Soit n un entier non nul. On considère l'espace $\mathbb{F}_q^{2n}$ muni de la forme alternée ω donnée par sa matrice $J_n=\left(\begin{smallmatrix}0 & -\mathrm{I}_n\\ \mathrm{I}_n & 0\end{smallmatrix}\right)$ dans la base canonique $(e_1,\dots,e_{2n})$. Le groupe symplectique sur $\mathbb{F}_q$ est le groupe qui stabilise cette forme :

$$\mathrm{Sp}_{2n}(\mathbb{F}_q)=\big\{A\in\mathrm{GL}_{2n}(\mathbb{F}_q),\ AJ_n\,{}^tA=J_n\big\}.$$

Un lagrangien, *voir aussi l'exercice VI-B.7, est un sous-espace de $\mathbb{F}_q^{2n}$ sur lequel ω est nulle et maximal pour cette propriété. On veut calculer le cardinal de l'ensemble $\mathscr{L}_n$ des lagrangiens de $\mathbb{F}_q^{2n}$. On pourra utiliser les résultats de l'exercice VI-B.7.*

1. *On note $\mathscr{C}$ l'ensemble des couples (u,v) de vecteurs de $\mathbb{F}_q^{2n}$ tels que $\omega(v,u)=1$ (les vecteurs u et v sont alors nécessairement indépendants). Montrer que le cardinal de $\mathscr{C}$ est égal à $(q^{2n}-1)q^{2n-1}$.*

   On peut choisir v dans $\mathbb{F}_q^{2n}$ non nul, puis u dans un hyperplan affine.

2. *Montrer que tout couple (u_1, v_1) de $\mathscr{C}$ peut être complété en une base $(u_1, u_2, \dots, u_n, v_1, v_2, \dots, v_n)$ où les couples (u_i, v_i) sont dans $\mathscr{C}$ et engendrent des plans deux à deux orthogonaux dans $\mathbb{F}_q^{2n}$. En déduire que $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ agit transitivement sur $\mathscr{C}$.*

3. *Montrer que pour cette action le stabilisateur d'un élément de $\mathscr{C}$ est isomorphe à $\mathrm{Sp}_{2n-2}(\mathbb{F}_q)$. En déduire la relation :*

$$\left|\mathrm{Sp}_{2n}(\mathbb{F}_q)\right| = q^{n^2} \prod_{k=1}^{n} (q^{2k} - 1).$$

4. *Montrer que $L_0 = \langle e_1, \dots, e_n \rangle$ est un lagrangien et que $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ agit transitivement sur $\mathscr{L}_n$.*

   C'est le résultat de l'exercice VI-B.7.

5. *Décrire le stabilisateur de L_0 dans $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ et en déduire la relation :*

$$|\mathscr{L}_n| = \prod_{k=1}^{n} (q^k + 1).$$

   Le stabilisateur est l'ensemble des matrices de la forme $A = \left(\begin{smallmatrix} M & X \\ 0_n & N \end{smallmatrix}\right)$ telles que $AJ_n\,{}^tA = J_n$, ce qui implique par un calcul simple : $N\,{}^tM = \mathrm{I}_n$, et $X\,{}^tM$ symétrique. On a donc :

$$|\mathscr{L}_n| = \frac{q^{n^2} \prod_{k=1}^{n} (q^{2k} - 1)}{q^{\frac{n(n+1)}{2}} \left|\mathrm{GL}_n(\mathbb{F}_q)\right|} = \prod_{k=1}^{n} (q^k + 1).$$

A.9. Exercice. *On garde les mêmes notations. On note $\mathrm{Gr}_{2,2n}$ la grassmannienne des plans de $\mathbb{F}_q^{2n}$ et $\mathbf{Gr}_{2,2n}$ l'ensemble des plans sur lesquels la forme ω est non dégénérée.*

1. *Montrer que l'application de $\mathscr{C}$ vers $\mathbf{Gr}_{2,2n}$ qui envoie le couple (u, v) sur le plan $\langle u, v \rangle$ engendré par u et v est surjective et que l'image réciproque d'un élément est de cardinal $q(q^2 - 1)$.*

2. *En déduire que l'on a : $|\,\mathbf{Gr}_{2,2n}\,| = q^{2n-2} \dfrac{q^{2n} - 1}{q^2 - 1}$.*

3. *Montrer que si F est un plan donné, alors $\omega|_F$ est soit nulle soit non dégénérée. En déduire que le nombre de plans sur lesquels ω est nulle est égal à $(1 + q + \cdots + q^{2n-3})(q^{2n} - 1)/(q^2 - 1)$.*

On utilise la formule du cardinal de la grassmannienne $\mathrm{Gr}(2, 2n)$ et l'on calcule $|\,\mathrm{Gr}(2, 2n)| - |\,\mathbf{Gr}(2, 2n)|$.

A.10. Exercice (Algèbre de Boole et géométrie symplectique sur $\mathbb{F}_2$)

Soit $E = \{1, \dots, n\}$ un ensemble fini et $\mathscr{P}(E)$ l'ensemble des parties de E. On rappelle que la différence symétrique et l'intersection munissent $V = \mathscr{P}(E)$ d'une structure d'anneau $(\mathscr{P}(E), \Delta, \cap)$. En particulier, on a une structure naturelle de $\mathbb{F}_2$-espace vectoriel $(V, \Delta, \cdot)$ avec le produit trivial par un élément de $\mathbb{F}_2$. On a $|V| = 2^n$ et donc $\dim_{\mathbb{F}_2} V = n$.

1. *Montrer que si A et B sont deux parties de l'ensemble E, alors on a : $|A \Delta B| = |A| + |B| \pmod 2$. En déduire que la forme ω définie par : $\omega(A, B) = |A \cap B| \pmod 2$ est bilinéaire et symétrique sur le $\mathbb{F}_2$-espace vectoriel $\mathscr{P}(E)$.*
2. *Montrer que l'ensemble V_0 des parties de cardinal pair est un hyperplan de V.*

   Astuss : c'est le noyau de la forme linéaire $A \mapsto |A| \pmod 2$.
3. *On suppose désormais n est pair, disons $n = 2m$. Montrer que le noyau de la restriction de ω à $V_0 \times V_0$ est la droite D engendrée par E. En déduire que ω passe au quotient sur l'espace-quotient $\overline{V}_0 = V_0/D$ et que la forme quotient $\bar{\omega}$ est non dégénérée.*
4. *Montrer que l'espace $\overline{V}_0$ possède $(2^{n-2} - 1)(2^{n-3} - 1)/3$ plans, parmi lesquels $(2^{n-4} - 1)(2^{n-2} - 1)/3$ sont totalement isotropes, et que la restriction de $\bar{\omega}$ à chacun des $2^{n-4}(2^{n-2} - 1)/3$ plans restants est non dégénérée.*

   On remarquera que ω est une forme symplectique [8] et l'on pourra appliquer l'exercice A.9.
5. *On suppose ici que l'on a : $n = 6$. Montrer que $\mathrm{Sp}_4(\mathbb{F}_2)$ agit sur les quinze paires d'éléments. Montrer que les 15 plans totalement isotropes de $\overline{V}_0$ sont de la forme $\{\emptyset, \{a, b\}, \{c, d\}, \{e, f\}\}$, où a, b, c, d, e et f sont distincts dans E. Montrer également que les 20 plans non totalement isotropes sont de la forme $\{\emptyset, \{a, b\}, \{a, c\}, \{b, c\}\}$, où a, b et c sont distincts dans E.*

Combinatoire quantique

A.11. Exercice (Récurrence pour les nombres binomiaux quantiques)

Soient m et n deux entiers tels que $1 \leqslant m \leqslant n$. Rappelez-vous de la preuve (ensembliste, et non pas calculatoire !) de l'incontournable formule de récurrence : $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$. Le but de l'exercice est de quantifier cette formule... et sa preuve.

[8] Wopop ! On est sur $\mathbb{F}_2$! Donc, symétrique implique antisymétrique, donc symplectique puisque non dégénérée.

1. *On fixe un espace E^- de dimension $n-1$ sur $\mathbb{F}_q$. On pose $E = E^- \oplus \mathbb{F}_q$. Soit F un sous-espace de E^- de dimension $m-1$ et soit $\mathrm{Gr}_F(E) = \{F' \in \mathrm{Gr}_m(E),\ F' \cap E^- = F\}$. On fixe un supplémentaire G de F dans E^-. Montrer que l'application*

$$g \mapsto \{(f + \alpha g, \alpha) \in E^- \oplus \mathbb{F}_q,\ f \in F, \alpha \in \mathbb{F}_q\}$$

définit une bijection de G sur $\mathrm{Gr}_F(E)$.

La réciproque est l'application qui envoie $F' \in \mathrm{Gr}_F(E)$ vers l'unique g tel que $(g,1) \in F'$.

2. *En déduire la formule :* $\begin{bmatrix} n \\ m \end{bmatrix}_q = \begin{bmatrix} n-1 \\ m \end{bmatrix}_q + q^{n-m} \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q$.

Lorsque F' dans $\mathrm{Gr}_m(E)$, de deux choses l'une : soit F' est inclus dans E^-, soit $F' \cap E^-$ est de dimension $n-1$. Il y a $\left[\begin{smallmatrix} n-1 \\ m \end{smallmatrix}\right]_q$ possibilités pour le premier cas et $q^{\dim G} \left[\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right]_q$ pour le second.

3. *En déduire une preuve alternative de la formule du binôme quantique (proposition 1.9) par récurrence sur n.*

A.12. Exercice (Convolution de Hall pour le dénombrement de variétés des drapeaux)

*Les techniques d'*algèbres de Hall *mêlent savamment catégories, théorie des représentations, géométrie algébrique et combinatoire. En voici une très modeste introduction. Ici donc, pas d'actions de groupes (en cas de manque, prendre son patch), mais des structures efficaces sur un fond sous-jacent de catégories.*

Soit $\mathscr{E}$ l'ensemble des sous-espaces vectoriels de $\mathbb{F}_q^n$ où n décrit $\mathbb{N}$. Soit Φ l'ensemble des fonctions F de $\mathscr{E}$ dans $\mathbb{N}$ satisfaisant à la propriété suivante :

Si V est un espace isomorphe à V', alors $F(V) = F(V')$.

On munit Φ de l'opération de convolution $*$ donnée par

$$(F * G)(V) = \sum_{0 \subset W \subset V} F(W) G(V/W) \quad \text{pour } F, G \in \Phi,\ V \in \mathscr{E},$$

où W parcourt l'ensemble des sous-espaces vectoriels de V.

Quitte à être redondant, on précise que $\subset$ désigne l'inclusion au sens large.

1. *(a) Montrer les formules suivantes pour F, G, H dans Φ*

$$\big((F * G) * H\big)(V) = \sum_{0 \subset X \subset W \subset V} F(X) G(W/X) H(V/W),$$

$$\big(F * (G * H)\big)(V) = \sum_{0 \subset X \subset W \subset V} F(X) G(W/X) H\big((V/X)/(W/X)\big),$$

où X, W décrivent l'ensemble des sous-espaces vectoriels de V tels que $X \subset W$.

(b) *Montrer que* $(V/X)/(W/X)$ *est isomorphe à l'espace-quotient* V/W. *En déduire :* $\big((F*G)*H\big)(V) = \big(F*(G*H)\big)(V)$.

2. *Pour tout* F *dans* Φ, *on note* $[F]$ *la* série formelle

$$\sum_{n\geqslant 0} F(\mathbb{F}_q^n)\frac{X^n}{[n]_q!}.$$

On pourra reconnaître ici une déformation quantique de l'exponentielle.

(a) *On fixe deux éléments* F, G *dans* Φ. *Démontrer la relation :*

$$(F*G)(\mathbb{F}_q^n) = \sum_{0\leqslant m\leqslant n} \big|\mathrm{Gr}_{m,n}(\mathbb{F}_q)\big|\, F(\mathbb{F}_q^m)G(\mathbb{F}_q^{n-m}).$$

(b) *Avec la formule du cardinal de la grassmannienne, en déduire que l'on a :* $[F*G] = [F]\,[G]$.

(c) *Démontrer à nouveau que la convolution est associative.*

3. *Pour* $k \geqslant 1$, *et* F *dans* Φ, *on définit* F^{*k} *de la manière suivante :* $F^{*1} = F$ *et, pour* $k \geqslant 1$, $F^{*k} = F^{*(k-1)} * F$ *(itéré* k *fois).*
Désormais, F *désigne l'élément de* Φ *tel que* $F(V) = 1$ *pour tout* V.
Pour tout espace V, *on note* $\mathscr{F}^k(V)$ *l'ensemble des drapeaux de sous-espaces à* k *sauts de* V, *défini par*

$$\mathscr{F}^k(V) = \big\{(V_1,\dots,V_k),\ 0\subset V_1\subset V_2\subset\cdots\subset V_k = V\big\}.$$

(a) *Montrer par récurrence que* $F^{*k}(V) = \big|\mathscr{F}^k(V)\big|$ *pour tout* V.

(b) *En calculant de deux façons la série* $[F^{*k}]$, *montrer la formule multinomiale quantique :*

$$\big|\mathscr{F}^k(V)\big| = \sum_{\substack{j_1,\dots,j_k\geqslant 0,\\ j_1+\cdots+j_k=n}} \frac{[n]_q!}{[j_1]_q!\cdots[j_k]_q!}.$$

On note R_V^k *la fraction rationnelle telle que* $R_V^k(q) = \big|\mathscr{F}^k(V)\big|$.

(c) *Montrer que* R_V^k *est bien définie et, en utilisant la formule (classique) du multinôme, que* $R_V^k(1) = \dim(V)^k$.

4. *De même, en utilisant* G *telle que* $G(V) = 1$ *si* $V \neq 0$ *et* $G(0) = 0$, *montrer*

$$\Big|\big\{(V_1,\dots,V_k),\ 0\subsetneq V_1\subsetneq V_2\subsetneq\cdots\subsetneq V_k\big\}\Big| = \sum_{\substack{j_1,\dots,j_k>0\\ j_1+\cdots+j_k=n}} \frac{[n]_q!}{[j_1]_q!\cdots[j_k]_q!}.$$

5. *On fixe une partie* P *de* $\mathbb{N}$ *et l'on considère la fonction* H *telle que* $H(V) = 1$ *si* $\dim V \in P$ *et* 0 *sinon. Quelle formule de cardinal obtient-on avec la même méthode ?*

Merci à Frédéric Chapoton pour avoir suggéré cet exercice.

Utilisation de polynômes générateurs

A.13. Exercice (Polynôme générateur et moyenne du nombre de cycles). *Soit n un entier naturel non nul. On considère le polynôme*

$$P_n = X(X+1)(X+2)\cdots(X+n-1).$$

Soit $c_n(\sigma)$ le nombre de cycles dans la décomposition en cycles disjoints de la permutation σ de $\mathfrak{S}_n$, en comptant les cycles de longueur 1. Ainsi, par exemple, on a : $c_n(e) = n$ où e est l'identité. Soit $R_n = \sum_{\sigma\in\mathfrak{S}_n} X^{c_n(\sigma)}$. On veut montrer que le nombre de permutations σ de $\mathfrak{S}_n$ telles que $c_n(\sigma) = k$ est égal au coefficient $a_{n,k}$ de X^k dans P_n, c'est-à-dire $R_n = P_n$.

1. *On fixe σ dans $\mathfrak{S}_n$.*
   (a) *Supposons que $\sigma(n) = n$ et soit $\sigma' \in \mathfrak{S}_{n-1}$ la restriction de σ à $\{1,\dots,n-1\}$. Montrer que $c_n(\sigma) - 1 = c_{n-1}(\sigma')$.*
   (b) *On suppose que $\sigma(n) = p$, où p est fixé dans $\{1,\dots,n-1\}$. Soit σ' dans $\mathfrak{S}_{n-1}$ obtenu à partir de la décomposition de σ en cycles disjoints en « retirant » n du cycle auquel il appartient*[9]*. Montrer que $c_n(\sigma) = c_{n-1}(\sigma')$.*
   (c) *Déduire de cette étude que $a_{n,k} = a_{n-1,k-1} + (n-1)a_{n-1,k}$.*
   Les deux termes correspondent aux deux cas étudiés. Pour le premier cas, c'est clair. Pour le second, il suffit de constater, qu'il y a $n-1$ choix de p possibles, et que pour chaque choix de p, la correspondance $\sigma \mapsto \sigma'$ est bijective : pour retrouver σ à partir de σ', il suffit de « rajouter » n après p dans le cycle concerné.
2. *Conclure que l'on a : $R_n = (X+n-1)R_{n-1}$, puis que l'on a : $R_n = P_n$.*

On retrouvera une déformation du polynôme P_n dans la théorie de Pólya, voir exemple V-5.9.

A.14. Exercice (Polynôme générateur des longueurs dans $\mathfrak{S}_n$)

Soit n un entier naturel non nul. On considère le polynôme

$$Q_n = (X^{n-1}+X^{n-2}+\cdots+1)(X^{n-2}+X^{n-3}+\cdots+1)\cdots(X+1) \in \mathbb{Z}[X].$$

On veut montrer que le nombre de permutations de longueur k dans $\mathfrak{S}_n$ est égal au coefficient de X^k dans Q_n.

1. *Soit $\mathbb{F}_q$ un corps fini de cardinal q et soit B le sous-groupe des matrices triangulaires supérieures de $G = \mathrm{GL}_n(\mathbb{F}_q)$. Montrer, avec l'exercice I-C.17, que l'orbite BwB de wB pour l'action par multiplication à gauche de B sur G/B est d'ordre $q^{\ell(w)}$.*

[9] Par exemple, si $\sigma = (134)(526)$ dans $\mathfrak{S}_6$, alors $n = 6$, $p = \sigma(6) = 5$ et $\sigma' = (134)(52)$

Par l'exercice I-C.17, le cardinal du stabilisateur est

$$(q-1)^n q^{\frac{n(n-1)}{2}-\ell(w)}.$$

2. *Conclure.*
   Il suffit de calculer, pour tout q, le cardinal de la variété des drapeaux G/B sur $\mathbb{F}_q$. On trouve la valeur de $Q_n(q)$, voir aussi [H2G2, proposition VIII-1.1], d'une part, par $|G/B| = |G|/|B|$ et, d'autre part, par la décomposition de Bruhat $\sum_{w\in\mathfrak{S}_n} q^{\ell(w)}$.

A.15. Exercice (Moyenne, variance et polynômes générateurs)

On va calculer la moyenne et la variance du nombre de cycles sur $\mathfrak{S}_n$, ainsi que la moyenne et la variance des longueurs. En fait, la chose est simple lorsque que l'on dispose d'une factorisation des polynômes générateurs.

Soit A un ensemble fini et soit f une application de A dans $\mathbb{N}$. On rappelle que la moyenne μ *et la* variance V *de f sont définies par :*

$$\mu = \frac{1}{|A|}\sum_{a\in A} f(a) \quad \textit{et} \quad V = \frac{1}{|A|}\sum_{a\in A}(f(a)-\mu)^2.$$

On introduit la série génératrice $P = \sum_{k\geqslant 0} a_k X^k \in \mathbb{Z}[X]$, où a_k est le cardinal de l'image réciproque $f^{-1}(k)$.

1. *Vérifier que P est un polynôme et que la moyenne est : $\mu = (\ln P)'(1)$.*
2. *Montrer que la variance est : $V = (\ln P)''(1) + (\ln P)'(1)$.*
   Vérifier que la variance est égale à $|A|^{-1}\sum_{a\in A} f(a)^2 - \mu^2$ et développer le calcul de $(\ln P)''(1) + (\ln P)'(1)$.
3. *Déduire de l'exercice A.13 que la moyenne et la variance du nombre de cycles sur $\mathfrak{S}_n$ sont respectivement*

$$1+\frac{1}{2}+\cdots+\frac{1}{n} \quad \textit{et} \quad \Big(1+\frac{1}{2}+\cdots+\frac{1}{n}\Big) - \Big(1+\frac{1}{2^2}+\cdots+\frac{1}{n^2}\Big).$$

   Le calcul de $\ln(P)$ et de ses dérivées est facilité par le fait que le polynôme P est factorisé.
4. *Déduire de l'exercice A.14 que la moyenne et la variance de la longueur sur $\mathfrak{S}_n$ sont respectivement $n(n-1)/4$ et (avec un peu de concentration) $n(n-1)(2n+5)/72$.*

Il est également intéressant de comparer à l'exercice X-B.17 pour l'interprétation de la moyenne et variance de certaines variables associées au calcul du nombre de points fixes pour des actions de groupes.

It looks like he was attempting to combine some kind of sorcery and scientific formula.
Guy Ritchie, *Sherlock Holmes*, 2009.

Chapitre V

Graphes et configurations

Dans la première partie du chapitre, nous allons tenter de sensibiliser le lecteur à la notion de configuration. Ici, le terme n'a pas vraiment le même sens que dans le chapitre III. Par « configuration », on entend la formalisation d'une situation géométrique sur les corps finis, où l'on dispose d'éléments appelés « points » regroupés en parties appelées « lignes » et possédant de belles propriétés de régularité, tant dans le nombre de points dans une ligne donnée que dans le nombre de lignes passant par un point donné.

Les mathématiques se font ici plus visuelles, contemplatives, ludiques et, disons-le, récréatives. Il ne sera pas ici question de classifier les configurations, ni d'en fournir un bestiaire, mais juste de les observer et de les construire dans un contexte donné.

Mais quel contexte ? On peut se douter que la géométrie affine ou projective sur un corps fini donne des exemples de configurations ; il est plus surprenant que la réduction des matrices sur un corps fini en fournisse de séduisantes, comme la fameuse configuration de Desargues.

On passera alors à une situation où ces objets sont particulièrement efficaces : la construction d'isomorphismes exceptionnels. En effet, une configuration dans un contexte donné (combinatoire, algèbre linéaire, géométrie des formes quadratiques, géométrie symplectique...) fournit une réalisation du groupe d'automorphismes de la structure (groupe symétrique, groupe linéaire, groupe orthogonal, groupe symplectique...) comme symétries combinatoires de la configuration. Ainsi, une même configuration provenant de deux contextes différents permet de comparer les groupes d'automorphismes de structures qui n'ont *a priori* pas de relation.

Lumineux, non ?

Pour donner quelques exemples illustrant ces méthodes vaudou, nous verrons que la configuration de Desargues permet de construire un isomorphisme $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ —ou, plus précisément, $\mathrm{PO}_3(\mathbb{F}_5) \simeq \mathfrak{S}_5$. Et le plan de Fano, configuration apparemment dominée par la sobriété mais dont le groupe d'automorphismes est tout de même d'ordre 168, sera la clé de l'isomorphisme $\mathrm{GL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. Enfin, nous verrons (en exercice) que la configuration de Cremona-Richmond apporte sur un plateau (technique, tout de même) l'isomorphisme $\mathrm{Sp}_4(\mathbb{F}_2) \simeq \mathfrak{S}_6$...

La partie suivante porte sur la distrayante combinatoire des coloriages. Partons de l'exemple du coloriage des faces du tétraèdre régulier par deux couleurs, disons rouge et vert. Il y a au départ 2^4 façons de colorier un tel tétraèdre et $\binom{4}{2}$ façons de le colorier avec deux faces rouges et deux faces vertes. Mais plusieurs coloriages sont « équivalents » : on peut alors compter les coloriages à isométrie positive du tétraèdre près. On ne trouvera alors plus que cinq façons de le colorier avec deux couleurs, dont une seule avec deux faces rouges et deux faces vertes.

La généralisation de ce problème est immédiate : on dispose d'un ensemble fini X muni d'un sous-groupe G du groupe $\mathfrak{S}(X)$ des permutations de X et l'on voudrait compter le nombre de coloriages « G-équivariants de X » avec un ensemble K de couleurs. On introduira le *polynôme indicateur de cycles* de G sur X et un théorème dû à Pólya apporte une réponse efficace au problème posé.

Ce théorème a de nombreuses applications : les coloriages des solides platoniciens ou le problème du collier de pierres sont attendues ; d'autres sont plus surprenantes, par exemple la combinatoire des arbres enracinés.

On verra enfin des problèmes de coloriage dans le cadre des configurations, dont certaines proviennent de la géométrie projective. Dans tous les cas, on se ramènera à un calcul du polynôme indicateur de cycles, ce qui conduira à l'étude des classes de conjugaison dans les groupes considérés (groupe linéaire, projectif, spécial linéaire...). Ce travail plus ~~fastidieux~~ technique sera reporté en annexe.

1. Configurations : exemples et définition

Voici un spécimen de mathématiques à la lyonnaise, transmis par la tradition orale depuis l'époque de Desargues, en même temps que la recette de la quenelle sauce canut que l'on peut déguster près du Gros Caillou.

Nous introduisons dans un premier temps la notion de configuration. Les configurations sont intéressantes en mathématiques de par leur ubiquité. Comme cela a été dit plus haut, elles permettent de construire des isomorphismes de groupes finis en réalisant de deux manières différentes une

configuration donnée et en identifiant les deux groupes de permutation ainsi obtenus. Et donc, de créer des ponts entre deux domaines, voire deux géométries.

C'est justement la démarche que l'on va adopter ici : le but de cette partie est de montrer que la géométrie projective permet de jolies configurations et en particulier, on réalisera la configuration $(10_3, 10_3)$ de Desargues en termes de matrices de trace nulle.

En géométrie affine ou projective, une *configuration* est un ensemble fini de points regroupés en un nombre fini ℓ de « lignes » (typiquement droites ou cercles), de sorte que par un point passe un nombre constant de lignes et qu'une ligne contienne un nombre fixe de points de la configuration. Il est judicieux, par simplicité et universalité, de s'affranchir de la géométrie et d'adopter la définition suivante.

1.1. Définition. Étant donnés des entiers n, ℓ, α et γ, une *configuration de type* (n_α, ℓ_γ) est un triplet $\mathscr{C} = (\mathscr{S}, \mathscr{L}, \mathscr{I})$ formé d'un ensemble $\mathscr{S}$ de cardinal n dont les éléments sont appelés *sommets* ou *points*, d'un ensemble $\mathscr{L}$ de cardinal ℓ dont les éléments sont appelés *lignes* ou parfois *droites* et d'une *relation d'incidence*[1], *i.e.* d'une partie $\mathscr{I} \subset \mathscr{S} \times \mathscr{L}$ soumis aux conditions ci-dessous. Lorsqu'un couple (p, L) appartient à $\mathscr{I}$, on dit que p et L sont incidents. On impose que :

(a) tout point est incident à exactement α lignes ;
(b) une ligne est incident à exactement γ points ;
(c) deux points sont incidents à au plus une ligne commune ;
(d) deux lignes sont incidents à au plus un point commun.

Voici en vrac du vocabulaire et des notations. Il arrive souvent que les éléments de $\mathscr{L}$ soient des parties de $\mathscr{S}$; l'incidence est alors simplement la relation d'appartenance d'un sommet $p \in \mathscr{S}$ à une partie $L \subset \mathscr{L}$. Par abus, pour des configurations générales, on dit qu'un sommet p *appartient à* une ligne L ou que L *contient* p pour indiquer que $(p, L) \in \mathscr{I}$. On dit que deux points sont *alignés* s'ils sont tous deux incidents à une même ligne.

Un *isomorphisme* entre deux configurations

$$\mathscr{C} = (\mathscr{S}, \mathscr{L}, \mathscr{I}) \quad \text{et} \quad \mathscr{C}' = (\mathscr{S}', \mathscr{L}', \mathscr{I}')$$

est la donnée de bijections entre les sommets et entre les lignes qui préserve l'incidence, c'est-à-dire de $\sigma : \mathscr{S} \to \mathscr{S}'$ et $\tau : \mathscr{L} \to \mathscr{L}'$ telles que pour $(p, L) \in \mathscr{S} \times \mathscr{L}$, on a : $(p, L) \in \mathscr{I}$ si et seulement si $\big(\sigma(p), \tau(L)\big) \in \mathscr{I}'$. Un *automorphisme* ou une *symétrie* d'une configuration $\mathscr{C}$ est un isomorphisme de $\mathscr{C}$ sur $\mathscr{C}$. Les automorphismes forment un groupe appelé *groupe de la configuration* (ou groupe des automorphismes ou groupe de symétries).

[1] C'est la notion antéduale de coïndicence.

La *configuration duale* de $\mathscr{C}=(\mathscr{S},\mathscr{L},\mathscr{I})$ est la configuration $\mathscr{C}^*=(\mathscr{L},\mathscr{S},{}^t\mathscr{I})$, où $(L,p)\in{}^t\mathscr{I}$ si et seulement si $(p,L)\in\mathscr{I}$. Une configuration est *autoduale* si elle est isomorphe à sa duale. La dualité est une involution sur l'ensemble des configurations et, par double inclusion, le groupe d'une configuration est égal au groupe de la configuration duale.

Un *drapeau* de $\mathscr{C}$ est un couple (p,L) formé par un sommet p incident à une ligne L. L'ensemble des drapeaux est $\mathscr{I}$, il caractérise la configuration.

1.2. Exemple. Un triangle peut être vu comme une configuration $(3_2,3_2)$. Plus généralement, un polygone à n sommets est une configuration (n_2,n_2). C'est une configuration autoduale et son groupe est le groupe diédral D_n.

1.3. Exemple. Le graphe complet sur 4 sommets (quatre points reliés entre eux de toutes les façons possibles) donne lieu à une configuration $(4_3,6_2)$. Sa duale (à droite) est appelée (trompeusement ?) quadrilatère complet. On vérifie que leur groupe de symétrie est le groupe $\mathfrak{S}_4$.

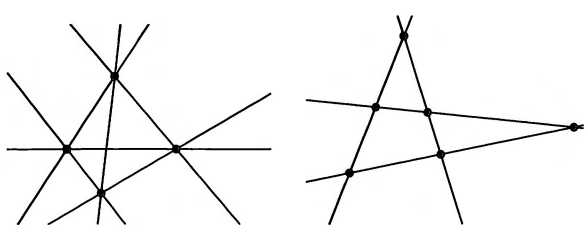


Figure 1.1. *Graphe complet* $(4_3,6_2)$ *et quadrilatère complet* $(6_2,4_3)$

1.4. Exemple. Il peut bien sûr y avoir plusieurs configurations de même type non isomorphes. La figure 1.2 donne les trois configurations de type $(9_3,9_3)$, dont celle de Pappus doit être familière ; la figure 1.3 montre deux des configurations de type $(10_3,10_3)$, dont celle de Desargues.

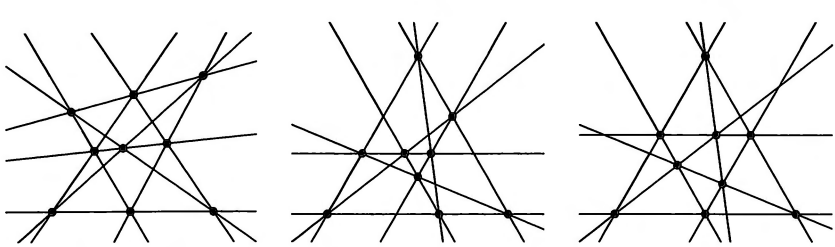


Figure 1.2. *Configurations* $(9_3,9_3)^{\text{Pappus}}$, $(9_3,9_3)^{\text{II}}$ *et* $(9_3,9_3)^{\text{III}}$

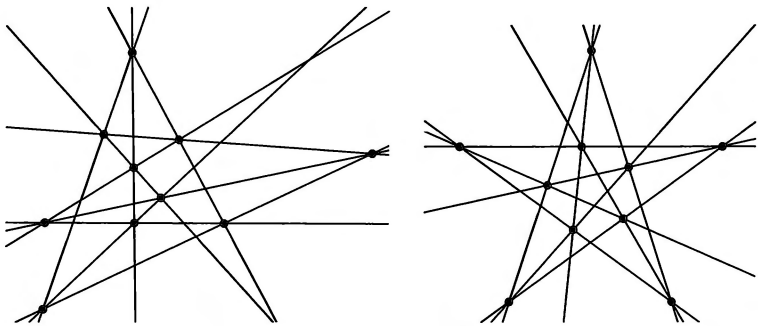


Figure 1.3. *Configurations* $(10_3, 10_3)^{\text{Desargues}}$ *et* $(10_3, 10_3)^{\text{exotique}}$

1.5. Remarque. On pourra au passage admirer la puissance du formalisme : on aurait pu plus concrètement définir une configuration comme un ensemble de « points » répartis en sous-ensembles appelés « lignes » plutôt que de construire deux ensembles et une relation d'incidence. Mais avec cette notion, plus instinctive, il aurait été très délicat de construire la configuration duale, alors que l'incidence est une relation qui se dualise sans aucun état d'âme.

1.6. Exercice. *Montrer que pour toute configuration finie de type* (n_α, ℓ_γ), *on a :*

$$n\alpha = \ell\gamma.$$

Calculer le cardinal de $\mathscr{I}$ « par lignes » et « par colonnes ».

1.7. Exercice (Espaces affine et projectif finis comme configurations)

Soient m *un entier et* q *le cardinal d'un corps fini* $\mathbb{F}_q$. *Montrer que les points de* $\mathbb{F}_q^m$ *et les droites affines forment une configuration de type* (n_α, ℓ_γ), *avec*

$$n = q^m, \quad \alpha = \frac{q^m - 1}{q - 1}, \quad \ell = \frac{q^{m-1}(q^m - 1)}{q - 1}, \quad \gamma = q.$$

Soit $\mathbb{P}^{m-1}(\mathbb{F}_q)$ *l'espace projectif de dimension* $m - 1$ *: un point (resp. une droite) est une droite vectorielle (resp. un plan vectoriel) de* $\mathbb{F}_q^m$. *Montrer que cela définit une configuration de type* (n_α, ℓ_γ), *avec*

$$n = \frac{q^m - 1}{q - 1}, \quad \alpha = \frac{q^{m-1} - 1}{q - 1}, \quad \ell = \frac{(q^m - 1)(q^{m-1} - 1)}{(q^2 - 1)(q - 1)}, \quad \gamma = q + 1.$$

On pourra faire agir le groupe projectif pour montrer que par un point passent le même nombre de droites. Le calcul de ℓ passe par l'exercice 1.6.

Pour $m = 3$, *montrer que le plan projectif est une configuration autoduale.*

On pourra fixer une forme non dégénérée sur $\mathbb{F}_q^3$ et utiliser l'orthogonalité.

1.8. Remarque (Automorphismes d'un espace projectif fini). Soient m un entier non nul, p un nombre premier et soit $\mathbb{P}^{m-1}(\mathbb{F}_p)$ l'espace projectif de l'exercice 1.7. Bien sûr, le groupe projectif $\mathrm{PGL}_m(\mathbb{F}_p)$ préserve l'incidence et l'alignement, donc il agit comme des automorphismes de la configuration. Le théorème appelé modestement « second théorème fondamental de la géométrie projective » [3, Theorem 2.26] exprime que le groupe des automorphismes de cette configuration est $\mathrm{PGL}_n(\mathbb{F}_p)$ pour $n \geqslant 3$.

Si l'on remplace le nombre premier p par une puissance q d'un nombre premier, le résultat change légèrement. Il faut remplacer le groupe des homographies $\mathrm{PGL}_n(\mathbb{F}_q)$ par le groupe des *semi-homographies*, c'est-à-dire le groupe des transformations de $\mathbb{P}^{m-1}(\mathbb{F}_q)$ provenant (par passage au quotient) des automorphismes *semi-linéaires* de $\mathbb{F}_q^m$. On rappelle qu'un automorphisme f de $\mathbb{F}_q^m$ est semi-linéaire si l'on a : $f(x+y) = f(x)+f(y)$ pour tous x et y de $\mathbb{F}_q^m$ et s'il existe un automorphisme σ du corps $\mathbb{F}_q$ tel que : $f(\lambda x) = \sigma(\lambda)f(x)$ pour tous λ de $\mathbb{F}_q$ et x de $\mathbb{F}_q^m$.

On voit donc qu'il y a une nuance entre les structures de « configuration projective » et d'« espace projectif ». Le groupe des automorphismes est plus gros pour la première que pour la seconde : le premier est le produit semi-direct du second par le groupe des automorphismes du corps — autrement dit, une semi-homographie est la composée d'une homographie et d'un automorphisme de corps agissant sur les coordonnées.

2. Configurations et conique nilpotente

Pour $\mathbb{K}$ un corps quelconque, on note $\mathfrak{sl}_2(\mathbb{K})$ l'hyperplan des matrices de trace nulle de $\mathscr{M}_2(\mathbb{K})$. Bien qu'un certain nombre des propriétés ci-dessous soient valables sur tout corps, on suppose que $\mathbb{K}$ est un corps fini $\mathbb{F}_q$ de cardinal q *impair*. On fixe un élément ζ de $\mathbb{F}_q$ qui n'est pas un carré.

On va relier la forme quadratique

$$Q = -\det$$

sur $\mathfrak{sl}_2(\mathbb{K})$ à la réduction des matrices.

2.1. Remarque. On peut trouver curieux, voire scandaleux, d'utiliser le déterminant comme forme quadratique. Est-ce un privilège de la dimension 2 ? Oui et non : le déterminant peut être vu comme un polynôme homogène et dont le degré est la dimension de l'espace, dans ce sens, il n'y a qu'en dimension 2 qu'il est une forme quadratique. Mais, cette forme quadratique se généralise facilement en toute dimension : la forme Q est en fait $A \mapsto \big(\mathrm{tr}(A^2) - \mathrm{tr}(A)^2\big)/2$. Dans le fond, l'omniprésence des formes de type « trace », sur les espaces de matrices carrées, provient du fait qu'elles sont invariantes pour l'action du groupe linéaire par conjugaison.

2.2. Proposition

(i) *Le discriminant*[2] *de Q vaut : $\delta(Q) = -1$.*

(ii) *Le cardinal du groupe orthogonal associé est :*

$$\big|\mathrm{O}(Q)\big| = 2(q-1)q(q+1)\,.$$

(iii) *Pour tout plan F de $\mathfrak{sl}_2(\mathbb{F}_q)$, il existe une base de F dans laquelle la matrice de la restriction Q a l'une des trois formes suivantes :*

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -\zeta \end{pmatrix}.$$

Ces cas s'excluent mutuellement.

Démonstration. (i) Via la base $(E_{11} - E_{22}, E_{12}, E_{21})$ (où les E_{ij} sont les matrices élémentaires), on identifie $\mathfrak{sl}_2(\mathbb{F}_q)$ à $\mathbb{F}_q^3$. La forme quadratique Q peut alors être vue comme $Q(a,b,c) = a^2 + bc$. Dans la base naturelle de $\mathbb{F}_q^3$, sa matrice est donc :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2^{-1} \\ 0 & 2^{-1} & 0 \end{pmatrix}.$$

Ainsi, son discriminant vaut : $\delta(Q) = -2^{-2} = -1 \in \mathbb{F}_q^*/\mathbb{F}_q^{*2}$.

(ii) C'est un cas particulier du théorème IV-2.1.

(iii) Soit donc F un plan quelconque de $\mathfrak{sl}_2(\mathbb{F}_q)$. Le rang de $Q|_F$ vaut (au plus 2 et) au moins 1, sinon on aurait : $F \subset F^\perp$, en contradiction avec : $\dim F^\perp = 3 - 2 = 1$, car Q est non dégénérée. Il reste deux cas.

Premier cas : $\operatorname{rg} Q|_F = 1$. Alors, par le classique procédé de Gauss (voir par exemple [H2G2, §V-B.3.1]) $Q|_F$ a pour matrice $\left(\begin{smallmatrix} 0 & 0 \\ 0 & \alpha \end{smallmatrix}\right)$ dans une base (e_1, e_2) de F avec $\alpha \neq 0$. De plus, $\dim\langle e_2\rangle^\perp = 2$ et, en choisissant $e_3 \in \langle e_2\rangle^\perp \setminus \langle e_1\rangle$, on obtient une base (e_1, e_2, e_3) de $\mathfrak{sl}_2(\mathbb{F}_q)$ dans laquelle la matrice de Q est de la forme

$$\begin{pmatrix} 0 & 0 & \beta \\ 0 & \alpha & 0 \\ \beta & 0 & \gamma \end{pmatrix},$$

pour β et γ scalaires convenables. Il vient : $-1 = \delta(Q) = -\beta^2\alpha$, ce qui prouve que α est un carré non nul. Soit donc a tel que $a^2 = \alpha$, alors, dans la base $(e_1, a^{-1}e_2)$, la matrice de $Q|_F$ est bien $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ comme désiré.

Deuxième cas : $\operatorname{rg} Q|_F = 2$. Par [H2G2, théorème V-1.2], la matrice de $Q|_F$ est congruente à $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ ou à $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \zeta \end{smallmatrix}\right)$, elles-mêmes congruentes à $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -\zeta \end{smallmatrix}\right)$, respectivement ou antirespectivement si -1 est un carré ou non.□

[2]Rappel : le discriminant d'une forme quadratique est le déterminant de l'une de ses matrices modulo les carrés, voir [H2G2, §V-A.1.9].

2.3. Notations. On note $\mathscr{T}$, $\mathscr{S}$, $\mathscr{E}$ l'ensemble des plans F de la proposition 2.2 qui admettent respectivement pour matrice $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1&0\\0&-\zeta\end{smallmatrix}\right)$ dans une base convenable.

2.4. Remarque. Un plan appartient à $\mathscr{T}$ (resp. $\mathscr{S}$, $\mathscr{E}$) si et seulement si le discriminant de la restriction à Q est 0 (resp. -1, $-\zeta$) dans $\mathbb{F}_q/(\mathbb{F}_q^*)^2$.

L'annexe A explique pourquoi $\mathscr{T}$ est l'ensemble des plans *tangents* au cône isotrope ; les plans de $\mathscr{S}$ sont *sécants* au cône le long de deux droites, ceux de $\mathscr{E}$ lui sont *extérieurs* (intersection réduite à l'origine).

2.5. Deux critères de réduction sur $\mathfrak{sl}_2(\mathbb{F}_q)$

Pour construire les configurations annoncées, on définit une partition :

$$\mathfrak{sl}_2(\mathbb{F}_q) = \mathscr{N}_0 \cup \mathscr{D}_0 \cup \mathscr{D}_0^*.$$

La partie $\mathscr{N}_0$ est le cône nilpotent ; par le théorème de Cayley-Hamilton, c'est le cône isotrope de la forme quadratique déterminant :

$$\mathscr{N}_0 = \{M \in \mathfrak{sl}_2(\mathbb{F}_q),\ Q(M) = 0\}.$$

On partitionne $\mathfrak{sl}_2(\mathbb{F}_q) \setminus \mathscr{N}_0$ en $\mathscr{D}_0 \cup \mathscr{D}_0^*$, où

$$\mathscr{D}_0 = \{M \in \mathfrak{sl}_2(\mathbb{F}_q),\ Q(M) \in (\mathbb{F}_q^*)^2\}, \quad \mathscr{D}_0^* = \{M \in \mathfrak{sl}_2(\mathbb{F}_q),\ Q(M) \notin (\mathbb{F}_q^*)^2\}.$$

On va donner maintenant deux interprétations aux ensembles $\mathscr{D}_0$ et $\mathscr{D}_0^*$, l'une en termes de réduction, et l'autre, en termes géométriques. On commence par la version « réduction ». Il est utile de remarquer que les valeurs propres d'une matrice de $\mathfrak{sl}_2(\mathbb{F}_q)$ sont opposées.

2.6. Proposition. *Soit M dans $\mathfrak{sl}_2(\mathbb{F}_q)$. Il est équivalent de dire :*

(i) $M \in \mathscr{D}_0$;

(ii) *le polynôme caractéristique χ_M de M est scindé à racines simples ;*

(iii) *la matrice M est diagonalisable et non nulle.*

Démonstration. Comme M est de trace nulle, on a : $\chi_M(X) = X^2 - Q(M)$. Si M appartient à $\mathscr{D}_0$, alors $Q(M)$ est un carré non nul donc χ_M a deux racines distinctes dans $\mathbb{F}_q$, d'où (i)⇒(ii). L'implication (ii)⇒(iii) est claire. Si M est diagonalisable et non nulle, son spectre est de la forme $\{-\lambda, \lambda\}$ (la trace est nulle) d'où : $Q(M) = \lambda^2$ et l'implication (iii)⇒(i). □

Ainsi, $\mathscr{D}_0$ est l'ensemble des matrices diagonalisables sur $\mathbb{F}_q$ et $\mathscr{D}_0^*$ est l'ensemble des matrices diagonalisables dans une extension quadratique[3] de $\mathbb{F}_q$, mais pas dans $\mathbb{F}_q$.

[3]Les valeurs propres sont les racines du polynôme caractéristique : si elles ne sont pas dans le corps $\mathbb{F}_q$, elles sont toutes deux dans une extension quadratique de $\mathbb{F}_q$.

La deuxième interprétation est inhabituelle aux yeux d'un lecteur « réel » : on voit l'ensemble $\mathscr{N}_0$ des matrices nilpotentes comme le cône isotrope de la forme quadratique $Q = -\det$ (la dimension est 2) ; l'ensemble $\mathscr{D}_0$ (resp. $\mathscr{D}_0^*$) est l'ensemble des points extérieurs (resp. intérieurs) à $\mathscr{N}_0$. Ici, un *point extérieur* (resp. *intérieur*) au cône est une matrice non nilpotente qui appartient à un plan tangent à $\mathscr{N}_0$ en un point non singulier (resp. qui n'appartient à aucun plan tangent). En version projective, si $\mathscr{N}$ désigne l'image de $\mathscr{N}_0$ dans le plan projectif $\mathbb{P}(\mathfrak{sl}_2(\mathbb{F}_q))$, un point extérieur à $\mathscr{N}$ est un point du plan projectif d'où l'on peut (resp. d'où l'on ne peut pas) mener une droite tangente à $\mathscr{N}$. La notion est détaillée dans l'annexe A.4.

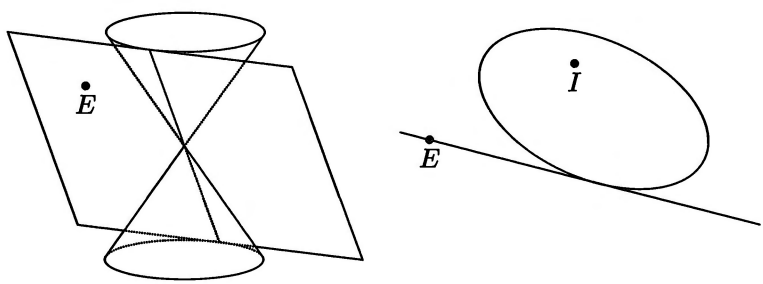


Figure 2.1. *Cône et conique avec un point extérieur (E) et un point intérieur (I)*

Même si elle ne servira pas tout de suite, cette interprétation géométrique mérite un peu d'attention.

2.7. Proposition. *Soit H une matrice non nulle de $\mathfrak{sl}_2(\mathbb{F}_q)$. Il est équivalent de dire :*

(i) *H est un point extérieur à $\mathscr{N}_0$;*

(ii) *la matrice H est diagonalisable et non nulle.*

Démonstration. (i)⇒(ii) Supposons que H est un point extérieur. Il appartient à la tangente à $\mathscr{N}_0$ en un point N non nul. Or, par la proposition A.3, l'espace tangent à $\mathscr{N}_0$ en N est l'espace des matrices M telles que $\Phi(N, M) = 0$, où Φ désigne la forme bilinéaire symétrique associée à Q. Ainsi, on a : $\Phi(N, H) = 0$. Puisque H n'est pas dans $\mathscr{N}_0$, la famille (N, H) est libre et la restriction de Q à l'espace engendré a pour matrice $\left(\begin{smallmatrix} 0 & 0 \\ 0 & \alpha \end{smallmatrix}\right)$. En particulier, $Q(H) = \alpha$ est un carré non nul d'après la proposition 2.2, donc H est diagonalisable par la proposition 2.6.

(ii)⇒(i) Si H est diagonalisable non nulle, alors, par la proposition 2.6, on a : $Q(H) = a^2$ pour $a \in \mathbb{F}_q^*$ convenable. Soit N_0 non nulle dans $\mathscr{N}_0$ et soit H_0 tel que (N_0, H_0) soit une base de l'espace tangent à $\mathscr{N}_0$ en N_0. Alors, par la proposition 2.2, $Q(H_0)$ est un carré non nul et donc, quitte

à multiplier H_0 par le bon scalaire, on peut supposer $Q(H_0) = Q(H)$. Le théorème de Witt ([H2G2, corollaire V-3.6]) assure qu'il existe g dans $\mathrm{O}(Q)$ tel que $g(H_0) = H$. Mais alors, de même que H_0 et N_0, $H = g(H_0)$ et $g(N_0)$ sont orthogonaux pour Q : cela signifie que H appartient au plan tangent à $\mathscr{N}_0$ en $g(N_0)$. □

Par construction, les ensembles $\mathscr{N}_0$, $\mathscr{D}_0$, $\mathscr{D}_0^*$ sont stables par multiplication par un scalaire non nul. On va noter $\mathscr{N}$ (resp. $\mathscr{D}$, $\mathscr{D}^*$) l'ensemble des droites vectorielles constituées d'éléments de $\mathscr{N}_0$ (resp. $\mathscr{D}_0$, $\mathscr{D}_0^*$) : ce sont des parties de $\mathbb{P}(\mathfrak{sl}_2(\mathbb{F}_q))$.

On peut maintenant dénombrer tous les ensembles rencontrés.

2.8. Proposition. *On a les égalités suivantes :*

(i) $|\mathscr{N}| = q+1$; $\quad |\mathscr{D}| = \frac{1}{2}q(q+1)$; $\quad |\mathscr{D}^*| = \frac{1}{2}(q-1)q$;

(ii) $|\mathscr{T}| = q+1$; $\quad |\mathscr{S}| = \frac{1}{2}q(q+1)$; $\quad |\mathscr{E}| = \frac{1}{2}(q-1)q$.

Démonstration. (i) Les matrices nilpotentes sont divisées en deux orbites pour l'action de $\mathrm{GL}_2(\mathbb{F}_q)$ par conjugaison : l'orbite nulle, singletonne, et l'orbite du bloc de Jordan $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ ([H2G2, théorème III-2.5.2]). Cette matrice admet pour stabilisateur (commutant) le sous-groupe $\left\{\left(\begin{smallmatrix}a&0\\b&a\end{smallmatrix}\right),\ a\in\mathbb{F}_q^*, b\in\mathbb{F}_q\right\}$. D'où :

$$|\mathscr{N}_0| = 1 + \frac{(q^2-1)(q^2-q)}{(q-1)q} = q^2,$$

ce que l'on a déjà vu au §IV-4. Il vient, en retirant la matrice nulle qui n'engendre pas de droite :

$$|\mathscr{N}| = \frac{q^2-1}{q-1} = q+1.$$

Calculons le cardinal de $\mathscr{D}_0$ en le décomposant en orbites comme précédemment : comme deux matrices diagonalisables sont semblables si et seulement si elles ont même spectre, les orbites sont classées par les paires de valeurs propres $\{\lambda, -\lambda\}$ ($\lambda \in \mathbb{F}_q^*$). Comme les deux valeurs propres sont distinctes, le stabilisateur de $\left(\begin{smallmatrix}\lambda&0\\0&-\lambda\end{smallmatrix}\right)$ est le sous-groupe $\left\{\left(\begin{smallmatrix}a&0\\0&b\end{smallmatrix}\right),\ a,b\in\mathbb{F}_q^*\right\}$. Il vient :

$$|\mathscr{D}_0| = \frac{q-1}{2}\,\frac{(q^2-1)(q^2-q)}{(q-1)^2} = \frac{1}{2}(q-1)q(q+1) \quad \text{et} \quad |\mathscr{D}| = \frac{1}{2}q(q+1).$$

Finalement, on obtient facilement par élimination :

$$|\mathscr{D}^*| = \frac{q^3 - |\mathscr{N}_0| - |\mathscr{D}_0|}{q-1} = \frac{(q-1)q}{2}.$$

(ii) Ces formules découlent d'une observation simple : l'orthogonalité en-

voie respectivement $\mathscr{N}$, $\mathscr{D}$, $\mathscr{D}^*$ sur $\mathscr{T}$, $\mathscr{S}$, $\mathscr{E}$ (et inversement !). En effet, supposons que x est dans $\mathscr{D}_0$, alors $Q(x)$ est un carré non nul, donc $\langle x\rangle^\perp$ est en somme directe avec $\langle x\rangle$. De plus, le discriminant de $Q|_{\langle x\rangle^\perp}$ est -1, ce qui implique que $x^\perp$ est dans $\mathscr{S}$ par la remarque 2.4. On vérifie de façon similaire qu'inversement, l'orthogonal d'un plan de $\mathscr{S}$ est une droite de $\mathscr{D}_0$. L'assertion sur $\mathscr{D}_0^*$ est similaire, et celle sur $\mathscr{N}_0$ en résulte par élimination (l'orthogonal d'un élément de $\mathscr{N}_0 \setminus \{0\}$ ne peut être ni dans $\mathscr{S}$ ni dans $\mathscr{E}$ d'après ce qui précède). □

2.9. Proposition. *Soit F un plan de $\mathfrak{sl}_2(\mathbb{F}_q)$. On a les égalités suivantes :*

$$|\mathscr{D}_0 \cap F| = \begin{cases} q^2-q & (F\in\mathscr{T}) \\ \dfrac{(q-1)^2}{2} & (F\in\mathscr{S}) \\ \dfrac{(q-1)(q+1)}{2} & (F\in\mathscr{E}) \end{cases} \qquad |\mathscr{D}_0^* \cap F| = \begin{cases} 0 & (F\in\mathscr{T}) \\ \dfrac{(q-1)^2}{2} & (F\in\mathscr{S}) \\ \dfrac{(q-1)(q+1)}{2} & (F\in\mathscr{E}). \end{cases}$$

Démonstration. Si F appartient à $\mathscr{T}$, alors dans une base (e_1, e_2) convenable, on a : $Q(\lambda e_1 + \mu e_2) = \mu^2$, donc $Q(x)$ est un carré non nul si et seulement si $x \in F \setminus \langle e_1\rangle$. D'où : $|\mathscr{D}_0 \cap F| = q^2 - q$ et $|\mathscr{D}_0^* \cap F| = 0$.

Si F est dans $\mathscr{S}$, alors on a : $Q(\lambda e_1 + \mu e_2) = \lambda^2 - \mu^2$ pour une base (e_1, e_2) convenable et $(\lambda, \mu) \in \mathbb{F}_5^2$, donc $Q(x)$ n'est pas nul si et seulement si x appartient à F privé de la réunion des deux droites isotropes. Il y a donc $q^2 - (2q-1) = (q-1)^2$ vecteurs de F tels que $Q(x)$ est non nul. Maintenant, les matrices $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ et $\zeta A = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & -\zeta \end{smallmatrix}\right)$ sont congruentes car elles ont même discriminant, donc il existe une matrice inversible P telle que ${}^tPAP = \zeta A$. Cela implique que $Q(Pu) = {}^t(PU)A(PU) = \zeta UAU = \zeta Q(u)$, et donc un vecteur u de F appartient à $\mathscr{D}_0$ si et seulement si Pu est dans $\mathscr{D}^*$. Comme P est bijective, il vient : $|\mathscr{D}_0 \cap F| = |\mathscr{D}_0^* \cap F| = (q-1)^2/2$.

Le cas où F appartient à $\mathscr{E}$ est similaire au précédent. □

2.10. Deux configurations dans $\mathbb{P}\,\mathfrak{sl}_2(\mathbb{F}_q)$

On arrive enfin à la construction des configurations promises. Dans le plan projectif $\mathbb{P}\,\mathfrak{sl}_2(\mathbb{F}_q)$, on considère les deux sous-configurations suivantes :

- la configuration $\mathscr{C}_q$ dont l'ensemble des points est $\mathscr{D}$ et l'ensemble des lignes est $\mathscr{S}$ (*i.e.* points extérieurs et droites sécantes à la conique $\mathscr{N}$) ; l'incidence d'un point et d'une ligne se traduit par l'inclusion de la droite dans le plan ;
- la configuration $\mathscr{C}'_q$ dont l'ensemble des points est $\mathscr{D}^*$ et l'ensemble des lignes est $\mathscr{E}$ (*i.e.* points intérieurs et des droites extérieures à $\mathscr{N}$) ; l'incidence d'un point et d'une ligne revient encore à l'inclusion de la droite dans le plan.

Les propositions précédentes entraînent que ce sont bien des configurations et l'on a immédiatement leurs types.

2.11. Corollaire. *Les configurations $\mathscr{C}_q$ et $\mathscr{C}'_q$ sont autoduales et de types respectifs*

$$\left(\binom{q+1}{2}_{\frac{q-1}{2}}, \binom{q+1}{2}_{\frac{q-1}{2}}\right) \quad \textit{et} \quad \left(\binom{q}{2}_{\frac{q-1}{2}}, \binom{q}{2}_{\frac{q-1}{2}}\right).$$

Démonstration. Par la proposition 2.8, on obtient le nombre de points et le nombre de lignes de la configuration. La proposition 2.9 montre que le nombre de points par ligne est constant. Comme $\mathscr{D}$ et $\mathscr{D}^*$ sont des cônes (privés de zéro), on doit diviser par $(q-1)$ pour passer du nombre de points non nuls au nombre de droites.

On a vu auparavant que l'orthogonalité échange les droites de $\mathscr{D}$ (resp. $\mathscr{D}^*$) avec les plans de $\mathscr{S}$ (resp. $\mathscr{E}$). On a donc le même nombre de lignes par point. Cela prouve que ce sont bien des configurations. De plus, comme $D \subset P$ implique $P^\perp \subset D^\perp$, ces configurations sont autoduales, l'automorphisme étant induit par l'orthogonalité. □

2.12. Triangles autopolaires

Il sera intéressant de grouper les points de certaines configurations pour construire des configurations plus petites. On peut toutefois sauter la fin de cette partie en première lecture et y revenir avec la motivation du corollaire 3.6.

2.13. Définition. Soit E un espace de dimension 3 et soit $\mathbb{P}(E)$ l'espace projectif associé. Soit Q une forme quadratique non dégénérée sur E et soit $\mathscr{N}$ la conique de $\mathbb{P}(E)$ d'équation $Q(u) = 0$. La *droite polaire*, ou simplement la *polaire* d'un point p de $\mathbb{P}(E)$ par rapport à la Q ou[4] à la conique $\mathscr{N}$ est la droite de $\mathbb{P}(E)$, image du plan de E orthogonal à la droite vectorielle p pour la forme Q. Voir l'annexe A.5 pour une description plus géométrique.

On appelle *triangle autopolaire* un triangle du plan projectif $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_q)$ tel que la polaire d'un sommet est la droite reliant les deux autres sommets, la polarité étant relative à la conique nilpotente $\mathscr{N}$.

On dit qu'un triangle autopolaire est *spécial* si c'est l'image d'une matrice de $\mathfrak{sl}_2(\mathbb{F}_q)$ dont le déterminant est un carré (c'est-à-dire un élément du groupe projectif spécial linéaire $\mathrm{PSL}_2(\mathbb{F}_q)$).

[4]On sait par le *Nullstellensatz* quadratique ([73, proposition XIII-2.1.1]) que sur un corps de cardinal strictement supérieur à 3, la conique $\mathscr{N}$ détermine Q à un scalaire multiplicatif près, ce qui rend la définition cohérente. Il y a un léger abus avec $\mathbb{F}_3$.

Comme la polarité n'est autre que l'orthogonalité et que la propriété d'être spécial est définie en termes de Q, le groupe $\mathrm{PO}(Q) = \mathrm{PGL}_2(\mathbb{F}_q)$ agit sur les triangles autopolaires spéciaux. Avant de les compter, faisons le lien entre la géométrie de la conique et les propriétés du groupe $\mathrm{PGL}_2(\mathbb{F}_q)$.

2.14. Lemme

(i) *Les points de* $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_q)\setminus\mathscr{N}$ *s'identifient aux involutions de* $\mathrm{PGL}_2(\mathbb{F}_q)$.

(ii) *Si* -1 *est (resp. n'est pas) un carré de* $\mathbb{F}_q$, *les involutions de* $\mathrm{PSL}_2(\mathbb{F}_q)$ *sont les points extérieurs (resp. intérieurs) de* $\mathscr{N}$.

(iii) *Deux involutions de* $\mathrm{PGL}_2(\mathbb{F}_q)$ *commutent si seulement si elles correspondant à deux droites de* $\mathfrak{sl}_2(\mathbb{F}_q)$ *qui sont orthogonales pour* Q.

Démonstration. (i) Par le théorème de Cayley-Hamilton, une matrice g de trace nulle satisfait à : $g^2 = Q(g)\mathrm{I}_2$. Par suite, elle est soit nilpotente, soit inversible et son image $[g] = \mathbb{F}_q^* g$ dans $\mathrm{PGL}_2(\mathbb{F}_q)$ est une involution.

Inversement, une involution provient d'une matrice g telle que g^2 est une homothétie. Autrement dit, g annule un polynôme $X^2 - \lambda$ pour $\lambda \in \mathbb{F}_q^*$. Si λ est un carré, g a pour valeurs propres opposées les racines de λ (g n'est pas une homothétie sinon $[g]$ serait l'identité dans PGL_2). Sinon, $X^2 - \lambda$ est irréductible sur $\mathbb{F}_q$ donc c'est le polynôme minimal de g donc aussi son polynôme caractéristique. Dans les deux cas, la trace de g est nulle.

(ii) Pour g dans $\mathrm{GL}_2(\mathbb{F}_q)$, la classe $[g]$ appartient à $\mathrm{PSL}_2(\mathbb{F}_q)$ si et seulement si le déterminant de g est un carré. Supposons la trace de g nulle. Lorsque -1 est un carré, il est équivalent de dire que $[g]$ appartient à $\mathrm{PSL}_2(\mathbb{F}_q)$, que $-Q(g)$ est un carré, que $Q(g)$ est un carré et que g (ou $[g]$) est un point extérieur (proposition 2.6). Si -1 n'est pas un carré, la correspondance est inversée car $Q(g)$ est un carré si et seulement si $-Q(g)$ n'en est pas un.

(iii) La forme bilinéaire Φ associée à $Q = -\det$ est : $\Phi(g,h) = \mathrm{tr}(gh)/2$ pour g et h dans $\mathfrak{sl}_2(\mathbb{F}_q)$. En effet, si l'on note λ et $-\lambda$ les valeurs propres (dans une clôture algébrique de $\mathbb{F}_q$) d'une matrice g de trace nulle, on a : $\Phi(g,g) = \mathrm{tr}(g^2)/2 = \lambda^2 = -\det(g) = Q(g)$.

Soient g et h deux matrices inversibles de trace nulle. Elles définissent des involutions $[g]$ et $[h]$ dans $\mathrm{PGL}_2(\mathbb{F}_q)$. Mézalor, il est équivalent de dire que $[g]$ et $[h]$ commutent et que $[gh]$ est une involution ; ou bien, grâce à (i), que l'on a : $\mathrm{tr}(gh) = 0$; ou encore, que g et h sont orthogonaux pour Q. □

2.15. Corollaire. *Un triangle autopolaire de* $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_q)$ *définit un sous-groupe de* $\mathrm{PGL}_2(\mathbb{F}_q)$ *isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^2$.

On constate donc que trois involutions qui commutent forment, avec le neutre, un sous-groupe de $\mathrm{PGL}_2(\mathbb{F}_q)$ isomorphe au groupe de Klein.

2.16. Proposition. *Dans le plan projectif* $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_q)$, *le nombre de triangles autopolaires spéciaux est* $q(q^2-1)/24$. *De plus, ils forment une seule orbite pour l'action de* $\mathrm{PGL}_2(\mathbb{F}_q)$.

Démonstration. Fixons un point $[g]$. Soit un point $[h]$ dans la polaire de $[g]$, il existe un unique triangle autopolaire dont $[g]$ et $[h]$ sont les sommets : le troisième sommet est l'intersection des polaires de $[g]$ et $[h]$. En effet, la polaire de ce troisième sommet est la droite reliant $[g]$ et $[h]$ (la relation « appartient à la polaire de » est symétrique car c'est l'orthogonalité). Si $[g]$ et $[h]$ sont des éléments de $\mathrm{PSL}_2(\mathbb{F}_q)$, le troisième aussi car c'est $[gh]$.

Supposons que -1 soit un carré. Alors les involutions de $\mathrm{PSL}_2(\mathbb{F}_q)$ sont les points extérieurs à $\mathscr{N}$. La polaire de $[g]$ est une droite sécante, elle contient $(q-1)/2$ points extérieurs par le corollaire 2.11. Cela montre que $[g]$ appartient à $(q-1)/4$ triangles autopolaires. Comme il y a 3 sommets par triangle et $q(q+1)/2$ points extérieurs (toujours le corollaire 2.11), le nombre de triangles autopolaires spéciaux est :

$$\frac{1}{3} \times \frac{q(q+1)}{2} \times \frac{q-1}{4} = \frac{q(q^2-1)}{24}.$$

Le cas où -1 n'est pas un carré est semblable : remplacer « point extérieur » par « point intérieur » et « sécante » par « droite extérieure ».

La transitivité de l'action de $\mathrm{PGL}_2(\mathbb{F}_q)$ est un peu plus délicate. Considérons d'abord le cas où -1 est un carré. Dans ce cas, une involution de $\mathrm{PSL}_2(\mathbb{F}_q)$ est la classe $[g_1]$ d'une matrice g_1 de trace nulle et de déterminant -1 qui est donc conjuguée à la matrice diagonale ayant pour valeurs propres 1 et -1 par un élément de $\mathrm{PGL}_2(\mathbb{F}_q)$. Un élément $g_2 = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ définit une involution $[g_2]$ de $\mathrm{PSL}_2(\mathbb{F}_q)$ qui commute à $[g_1]$ si et seulement si $0 = \mathrm{tr}(g_1 g_2) = 2a$ et $-bc = 1$. Ainsi, on a : $a = 0$ et, quitte à remplacer g_2 par $b^{-1}g_2$, on peut supposer que l'on a : $b = -1$. Cela montre que le sous-groupe engendré par $[g_1]$ et $[g_2]$ est dans l'orbite sous $\mathrm{PGL}_2(\mathbb{F}_q)$ de celui engendré par $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ et $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$.

Passons au cas où -1 n'est pas un carré. On dispose alors d'une racine carrée i de -1 dans $\mathbb{F}_{q^2}$. Soient g_1, g_2, h_1, h_2 des éléments de $\mathrm{SL}_2(\mathbb{F}_q)$ tels que $\big([g_1],[g_2]\big)$ et $\big([h_1],[h_2]\big)$ soient deux couples d'involutions de $\mathrm{PSL}_2(\mathbb{F}_q)$ qui commutent l'une avec l'autre. D'après le cas précédent, il existe une matrice inversible $p \in \mathrm{GL}_2(\mathbb{F}_{q^2})$ dont la classe $[p]$ dans le groupe projectif conjugue $[g_1]$ en $[h_1]$ et $[g_2]$ en $[h_2]$. Il existe donc un scalaire α_1 de $\mathbb{F}_{q^2}$ tels que l'on ait : $pg_1p^{-1} = \alpha_1 h_1$. Par le lemme 2.14 et sa preuve, les spectres de g_1 et h_1 sont tous deux égaux à $\{-i, i\}$ donc α_1 vaut ± 1. De même, on a : $pg_2p^{-1} = \pm h_2$.

À présent, en reprenant l'argument de [H2G2, proposition III-4.1], écrivons p sous la forme : $p = r + is$, où r et s sont deux matrices à coefficients

dans $\mathbb{F}_q$, et notons $p(t) = r + zs$, où z est une indéterminée. Le polynôme $f(z) = \det p(z)$ est non nul (car $f(i) \neq 0$) et, vu son degré, il a au plus 2 racines dans $\mathbb{F}_q$. Comme on est sur un corps de cardinal impair $q \geqslant 3$, il existe $t_0 \in \mathbb{F}_q$ tel que $p_0 = p(t_0)$ appartient à $\mathrm{GL}_2(\mathbb{F}_q)$. L'égalité $pg_1 = \alpha_1 h_1 p$ (avec $\alpha_1 = \pm 1$) donne : $rg_1 = \alpha_1 h_1 r$ et $sg_1 = \alpha_1 h_1 s$, puis : $p_0 g_1 = \alpha_1 g_1 p_0$ et $[p_0][g_1][p_0]^{-1} = [h_1]$. De même : $[p_0][g_2][p_0]^{-1} = [h_2]$. On peut conclure. □

2.17. Remarque. Étant donné deux involutions qui commutent, une autre involution qui leur commute est nécessairement sur l'intersection des deux polaires. Cela montre que les 2-sous-groupes abéliens élémentaires (*i.e.* isomorphes à $(\mathbb{Z}/2\mathbb{Z})^r$ pour r convenable) maximaux de $\mathrm{PSL}_2(\mathbb{F}_q)$ sont d'ordre 4. Les sous-groupes de ce type sont précieux pour comprendre les représentations des groupes finis quand la caractéristique divise l'ordre du groupe.

3. Cas particulier : configuration de Desargues

Il y a cinq, Saint-Michel et Saint-Jean,
les cinq doigts de la main et puis Cincinnati.
Michel Polnareff, *Y a qu'un ch'veu*, 1968.

Attardons-nous sur le cas particulier où $q = 5$. La seconde configuration $\mathscr{C}_5'$ est donc de type $(10_3, 10_3)$. Il s'agit de la configuration de Desargues ([H2G2, §XI-2] et figure 3.1). Nous en donnons ici une brève explication sans rentrer dans les détails fastidieux de la preuve : parmi les configurations $(10_3, 10_3)$, une seule possède un groupe d'automorphismes transitif sur les drapeaux, *i.e.* l'ensemble des couples formés d'un point et d'une ligne qui le contient, voir [38]. Or, les configurations précédentes satisfont à cette propriété : c'est une conséquence du théorème de Witt.

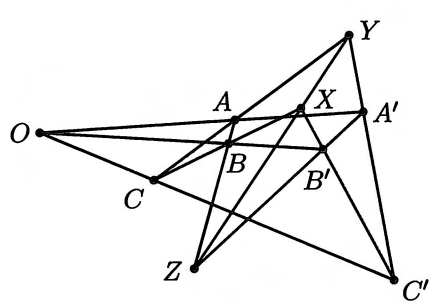


Figure 3.1. *Construction de la configuration de Desargues*

Déterminons le groupe G de la configuration de Desargues (figure 3.1).

3.1. Lemme. *L'ordre du groupe de G est au plus* 120.

Démonstration. Pour l'image de O par un élément de G, on a au maximum dix possibilités (tous les sommets possibles), en supposant que l'on a choisi O, l'image de A doit être alignée avec O et distincte de O, d'où au maximum six possibilités dans $\{A, B, C, A', B', C'\}$; supposons maintenant que l'on ait choisi A, alors l'image de B doit être alignée avec O et A, et distincte de ces points. Il ne reste plus que deux possibilités au maximum : B et C. Si l'on suppose que c'est B, on voit que tous les autres points doivent être fixés. D'où : $|G| \leqslant 10 \times 6 \times 2 = 120$. □

3.2. Lemme. *Le groupe G est isomorphe à* $\mathrm{PO}(Q) = \mathrm{O}(Q)/\{\pm \mathrm{Id}\}$.

Démonstration. Maintenant, la réalisation de la configuration de Desargues comme $\mathscr{C}_5'$ montre que $\mathrm{O}(Q)$ agit sur la configuration. En effet :

- les sommets sont des classes de matrices M (modulo homothéties) telles que $Q(M)$ n'est pas un carré ; le groupe $\mathrm{O}(Q)$ stabilise donc l'ensemble des points de la configuration ;
- les lignes de la configuration correspondent aux plans P tels que le discriminant de $Q|_P$ est égal à -1 ; le groupe $\mathrm{O}(Q)$ stabilise donc l'ensemble des lignes de la configuration ;
- si $g \in \mathrm{O}(Q)$ et $p \in \ell$, alors, il est clair que $g(p) \in g(\ell)$, car g respecte l'inclusion.

Toutefois, l'action de $\mathrm{O}(Q)$ sur $\mathbb{P}^2 = \mathbb{P}\mathfrak{sl}_2(\mathbb{F}_5)$ n'est pas fidèle : les homothéties agissent trivialement. Réciproquement, supposons que $g \in \mathrm{O}(Q)$ stabilise les dix sommets de la configuration, il stabilise donc un repère projectif (quatre points dont trois quelconques d'entre eux ne sont pas alignés, par exemple O, A, B, C) et donc comme g est dans le groupe linéaire, le premier théorème fondamental de la géométrie projective, voir [H2G2, proposition X-1.2.7], dit qu'il s'agit d'une homothétie. Comme g est dans $\mathrm{O}(Q)$, il vaut $\pm \mathrm{Id}$. Ainsi, le groupe $\mathrm{PO}(Q) = \mathrm{O}(Q)/\{\pm \mathrm{Id}\}$ s'injecte dans G.

On a d'après la proposition 2.2 : $|\mathrm{PO}(Q)| = 2(5-1)5(5+1)/2 = 120$. C'est le nombre rêvé qui nous permet de conclure que $\mathrm{PO}(Q)$ est le groupe d'automorphismes de la configuration. □

3.3. Configuration de Desargues à partir de cinq points

Voici une autre façon de réaliser la configuration de Desargues (figure 3.2). Dans l'espace, on fixe un plan Π (figuré par le parallélogramme grisé) et cinq points notés $A_1, \ldots, A_5$ ou plus simplement $1, \ldots, 5$. On les choisit en position suffisamment générale pour que toutes les intersections mentionnées plus bas existent. On définit les $\binom{5}{2}$ points de la configuration : le point A_{ij}, ou (ij), est l'intersection de Π et de la droite (A_iA_j) $(i, j$

distincts). Puis les dix lignes de la configuration : la droite D_{ijk}, ou (ijk), est l'intersection de Π et du plan $(A_iA_jA_k)$ (i, j, k distincts).

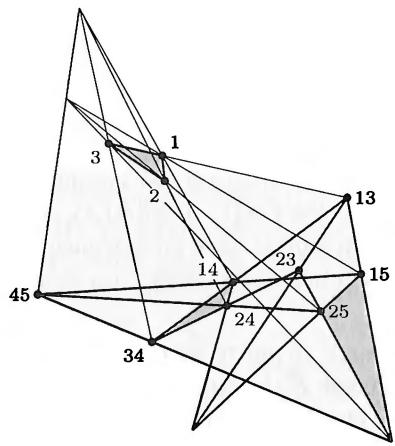


Figure 3.2. *Configuration de Desargues vue comme projection*

(On voit par exemple que les triangles $A_{14}A_{24}A_{34}$ et $A_{15}A_{25}A_{35}$, anciennement ABC et $A'B'C'$, sont les projections centrales sur Π du triangle $A_1A_2A_3$ depuis A_4 et A_5.)

Ainsi, toute permutation des cinq points $\{1,2,3,4,5\}$ fournit un élément du groupe de la configuration de Desargues. L'action de $\mathfrak{S}_5$ sur la configuration est une réalisation de l'action naturelle sur les parties à deux éléments (les points) et trois éléments (les lignes). L'incidence d'un point sur une ligne traduit l'inclusion, elle est préservée par permutation. Autrement dit, on vient de décrire un morphisme $\iota : \mathfrak{S}_5 \to G$.

(Dualement, on peut partir de cinq plans en position générale. Les $\binom{5}{2}$ droites d'intersection de deux des plans et les $\binom{5}{3}$ points d'intersection de trois des plans sont dans la configuration de Desargues. On voit bien comment passer d'une réalisation à l'autre — non ?)

Du fait que le seul sous-groupe distingué non trivial de $\mathfrak{S}_5$ est $\mathfrak{A}_5$, on déduit que ι est injectif. En effet, le noyau de ι est trivial ou contient $\mathfrak{A}_5$. Or, s'il contenait $\mathfrak{A}_5$, l'image de l'action aurait au plus un élément non trivial ; on voit en regardant l'image de (12) et (34) qu'il n'en est rien.

Les égalités $|\mathfrak{S}_5| = 120 = |G|$ donne aussi la surjectivité et il s'agit donc d'un isomorphisme. On a donc prouvé le théorème suivant.

3.4. Théorème. *On a un isomorphisme exceptionnel :*

$$\mathrm{PO}_3(\mathbb{F}_5) \simeq \mathfrak{S}_5.$$

Ces deux groupes sont des réalisations du groupe des automorphismes de la configuration de Desargues.

3.5. Corollaire. *On a des isomorphismes exceptionnels :* $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ *et* $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

Démonstration. L'action de $\mathrm{GL}_2(\mathbb{F}_5)$ par conjugaison sur $\mathfrak{sl}_2(\mathbb{F}_5)$ préserve le déterminant, puisque $\det(PAP^{-1}) = \det(A)$, donc elle préserve la forme quadratique Q. L'action fournit donc un morphisme de $\mathrm{GL}_2(\mathbb{F}_5)$ dans $\mathrm{O}(Q)$, puis, en considérant l'action sur $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_5)$, un morphisme de $\mathrm{GL}_2(\mathbb{F}_5)$ dans $\mathrm{PO}(Q)$.

Montrons que le noyau de ce morphisme est réduit aux homothéties. Il suffit de voir que tout élément P du noyau fixe toute droite de $\mathbb{F}_5^2$. Supposons, par l'absurde, que P envoie une droite D de $\mathbb{F}_5^2$ sur une droite D' distincte de D. Soit D'' une droite du plan $\mathbb{F}_5^2$ distincte de D et de D'. On construit un élément A de $\mathfrak{sl}_2(\mathbb{F}_5)$ qui a pour droite propre D (resp. D'') avec valeur propre 1 (resp. -1). Par hypothèses, $P^{-1}AP = \mu A$, pour un $\mu \in \mathbb{F}_5^*$. Alors, P envoie un vecteur v de D, sur un vecteur propre de A de valeur propre μ, et donc P envoie v sur un vecteur propre, donc sur un vecteur de D ou de D''. Absurde, puisque D' est distincte de ces deux droites.

L'action fournit donc un morphisme injectif de $\mathrm{PGL}_2(\mathbb{F}_5)$ dans $\mathrm{PO}_3(\mathbb{F}_5)$ et donc surjectif par cardinalité. On obtient l'isomorphisme $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$. L'autre isomorphisme en découle en prenant les groupes dérivés. □

« De quoi qu'y a cinq ? » demandait l'enfant avant Michel Polnareff. C'est là que servent les triangles autopolaires (2.13 et 2.16).

3.6. Corollaire. *Il y a cinq triangles autopolaires spéciaux dans* $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_5)$.

Cette approche fort élégante de la configuration de Desargues nous a été indiquée par Paul Gérardin il y a fort longtemps. Les amateurs qui voudront passer de 5 à 7 s'intéresseront à l'exercice D.5 sur $\mathbb{F}_7$.

3.7. Remarque. C'est un bon moment pour faire les exercices D.9 à D.11 sur la *configuration de Cremona-Richmond.* À l'instar de la configuration de Desargues, elle possède deux réalisations, l'une combinatoire et l'autre en termes de géométrie symplectique, ce qui met en évidence un isomorphisme exceptionnel : $\mathfrak{S}_6 \simeq \mathrm{Sp}_4(\mathbb{F}_2)$. De plus, on retrouve très naturellement dans ce contexte l'automorphisme extérieur de $\mathfrak{S}_6$. Les méthodes sont très analogues à celles que l'on vient de rencontrer.

4. Chaînes de Clifford

Be wise! Generalize!
Cité par Michael Artin, *Algebra*, 1991

And so on!
Donald Coxeter, *Introduction to geometry*, 1961

4.1. Présentation

Le point de départ est un théorème attribué à Wallace en 1806 (d'après [22]), étendu une première fois par Miquel [57] puis en une chaîne infinie de théorèmes par Clifford [17] en 1871. On part d'un point $A_\emptyset$ et de quatre cercles-ou-droites $C_1, \dots, C_4$ contenant $A_\emptyset$. Pour i et j distincts, l'intersection $C_i \cap C_j$ contient $A_\emptyset$ et un autre point A_{ij}. Pour i, j, k distincts, on note C_{ijk} le cercle contenant A_{ij}, A_{jk} et A_{ki}. Le fait est que les quatre cercles C_{ijk} ont un point commun noté A_{1234}, parfois appelé *point de Wallace* ou *point de Miquel* (lorsque $A_\emptyset$ est à l'infini, les C_i sont des droites et définissent un quadrilatère complet).

Dans la figure 4.1, on note l'ensemble des indices par la fonction indicatrice de la partie correspondante. Ainsi : $A_\emptyset = 0000$, $C_1 = 1000$, etc., $A_{13} = 1010$, etc., $C_{124} = 1101$, etc. et $A_{1234} = 1111$.

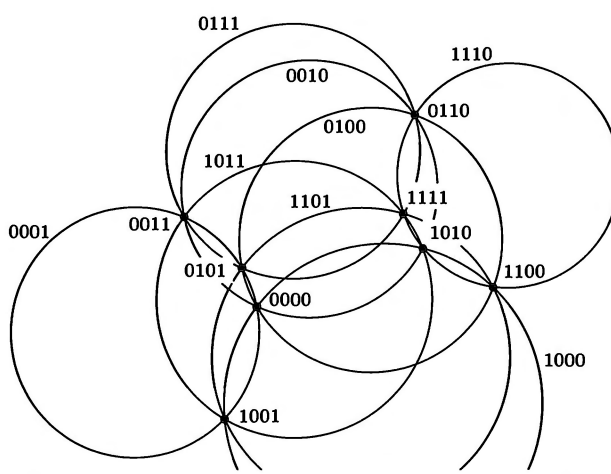


Figure 4.1. *Configuration de Miquel, de Clifford ou de Möbius d'ordre* 4

Démontrons-le à l'aide de la formule des six birapports ([4, exercice VI-40] ou [H2G2, proposition X-1.22]). On note $I = \{1, 2, 3, 4\}$ et l'on définit A_{1234} comme le second point d'intersection des cercles C_{234} et C_{134}, le premier étant A_{12}. On montre d'abord que A_{1234} appartient à C_{124}. On dispose des points au sommet d'un cube comme dans la figure 4.2.

Chaque face du cube détermine un birapport et le produit des six birapports vaut 1. Or quatre points sont cocycliques ou alignés si et seulement si leur birapport est réel. Par hypothèse, les points disposés sur cinq des six faces du cube sont cocycliques : par exemple, les points $A_\emptyset$, A_{12}, A_{13}, A_{14} sont sur le cercle C_1 ; les points A_{13}, A_{14}, A_{34}, A_{1234} sur le cercle C_{134}, etc. Il en résulte que le birapport associé à la sixième face est réel : autrement dit, le point A_{1234} appartient au cercle C_{124} contenant A_{12}, A_{14} et A_{24}. En permutant les rôles de 3 et 4, on montre qu'il appartient aussi à C_{123}.

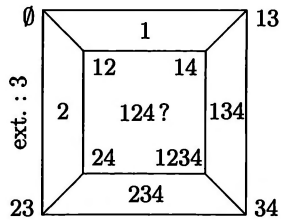


Figure 4.2. *Six birapports pour le théorème de Miquel*

On obtient ainsi une configuration formée des huit points A_I (I partie de cardinal pair de $\{1,2,3,4\}$) et des huit lignes C_J (J partie de cardinal impair). Elle est de type $(8_4, 8_4)$ et possède un gros groupe de symétries que l'on va découvrir. La « chaîne de théorèmes » de Clifford ([19, §14.9]) montre comment former, à partir d'un nombre quelconque n de cercles initiaux, une configuration analogue de type $\left((2^{n-1})_n, (2^{n-1})_n\right)$.

4.2. Proposition (Configuration de Clifford). *Soit n un entier. On définit une configuration de points et de cercles indexée par les parties de $\{1,\dots,n\}$ par récurrence sur le cardinal de la partie. Pour commencer, $A_\emptyset$ est un point arbitraire du plan et $C_1,\dots,C_n$ des cercles contenant $A_\emptyset$, en position générale sous cette contrainte. Soit I une partie de cardinal au moins 2 :*

– si $|I|$ est pair, les cercles $C_{I\setminus\{k\}}$ ($k \in I$) ont un point commun A_I ;

– si $|I|$ est impair, les points $A_{I\setminus\{k\}}$ ($k \in I$) sont sur un même cercle C_I.

La configuration ainsi définie est isomorphe à la configuration des parties de $\{1,\dots,n\}$ de 4.3.

La figure 4.3 montre la configuration pour les petites valeurs de n avec des notations analogues à la figure 4.1.

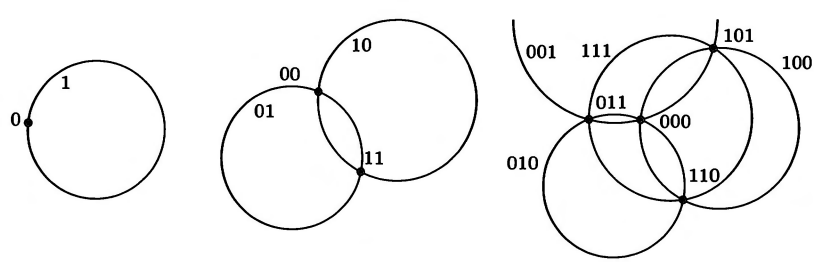
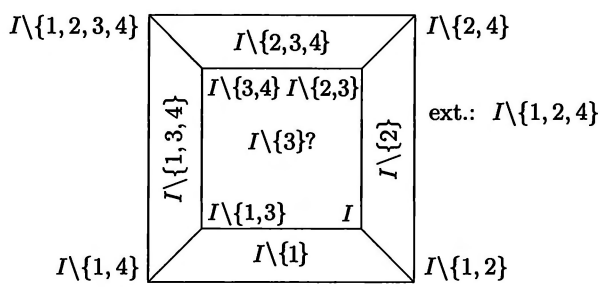


Figure 4.3. *Configurations de Clifford d'ordres* 1, 2 *et* 3

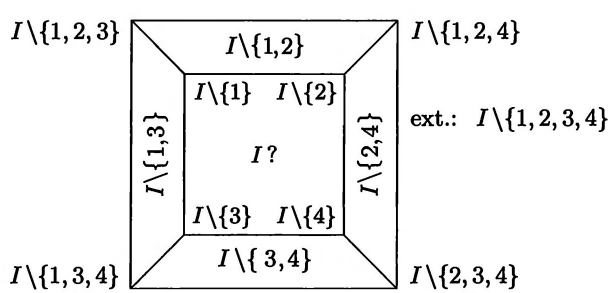
Démonstration. Pour une partie à 2 éléments $I = \{i, j\}$, on note A_I le point d'intersection de C_i et C_j autre que $A_\emptyset$. Pour $J = \{i, j, k\}$ partie à 3 éléments, on note C_J le cercle contenant les points A_{ij}, A_{jk} et A_{ki}.

On suppose désormais que n vaut au moins 4. Par récurrence sur le cardinal d d'une partie I, on construit un point A_I si $|I|$ est pair ou un cercle C_I si $|I|$ est impair. La récurrence a été amorcée pour $d \leqslant 3$. Soit d supérieur à 4 et supposons que la construction ait été menée pour toutes les parties de cardinal au plus $d - 1$.

Premier cas : d est pair. On montre que pour toute partie I à d éléments, les cercles $C_{I\setminus\{k\}}$ $(k \in I)$ ont un point commun noté A_I. On choisit deux éléments de I que l'on note 1 et 2 et l'on définit A_I comme l'intersection de $C_{I\setminus\{1\}}$ et de $C_{I\setminus\{2\}}$ qui n'est pas $A_{I\setminus\{1,2\}}$. On fixe deux autres éléments de I, notés arbitrairement 3 et 4. Grâce au cube suivant, on montre que A_I appartient à $C_{I\setminus\{3\}}$. De même, on montre que A_I appartient à $C_{I\setminus\{4\}}$ en permutant les rôles de 3 et 4.



Deuxième cas : d est impair. On fixe trois éléments notés arbitrairement 1, 2 et 3 dans I et l'on définit C_I comme le cercle qui contient les points $A_{I\setminus\{1\}}$, $A_{I\setminus\{2\}}$ et $A_{I\setminus\{3\}}$. Il reste à montrer que pour un élément quelconque de I, noté 4 par exemple, le point $A_{I\setminus\{4\}}$ appartient à C_I. Pour cela, on forme un cube.



Cinq faces correspondent à des points cocycliques (la partie qui décrit le cercle est inscrite au milieu de la face) donc la sixième, celle marquée « I ? », correspond à des points cocycliques. De plus, si $|I|$ et $|J|$ sont tous deux inférieurs à d, A_I appartient à C_J lorsque $|I\triangle J| = 1$. La construction se termine par un point ou un cercle selon que n est pair ou impair. □

4.3. Parties de $\{1,\dots,n\}$ et configuration de Möbius

On identifie l'ensemble des parties de $\{1,\dots,n\}$ à l'espace vectoriel $E = (\mathbb{Z}/2\mathbb{Z})^n$: si $(e_i)_{1\leqslant i\leqslant n}$ est la base canonique de E, une partie I est identifiée à $e_I = \sum_{i\in I} e_i$. La somme de E réalise la différence symétrique :

$$e_I + e_J = e_{I\triangle J}, \quad \text{où} \quad I\triangle J = (I\cup J)\setminus(I\cap J).$$

On considère la configuration dont les points sont les parties I ayant un nombre *pair* d'éléments et les lignes sont les parties J ayant un nombre *impair* d'éléments. Comme on a : $(1-1)^n = 0$, il y a 2^{n-1} parties de chaque parité.

On dit qu'un point I est incident à une ligne J si I et J diffèrent exactement d'un élément, c'est-à-dire si $|I\triangle J| = 1$; cela revient à dire que la distance de Hamming[5] de e_I et e_J vaut 1 ou que $e_I = e_J + e_k$ pour un certain $k \in \{1,\dots,n\}$. Un point (resp. une ligne) I est donc incident(e) aux n lignes (resp. points) $I\triangle\{k\}$ où k décrit $\{1,\dots,n\}$.

On obtient donc une configuration de type $\big((2^{n-1})_n, (2^{n-1})_n\big)$, appelée *configuration de Möbius* suivant [68, §5.3.7]. La configuration de Clifford en est une réalisation géométrique. On va déterminer le groupe de symétries de ces configurations isomorphes.

4.4. Notations. Soit n un entier non nul. On note B_n le produit semi-direct $\mathfrak{S}_n \ltimes (\mathbb{Z}/2\mathbb{Z})^n$, où $\mathfrak{S}_n$ agit sur $E = (\mathbb{Z}/2\mathbb{Z})^n$ par permutation des coordonnées. On note D_n le sous-groupe d'indice 2 de B_n formé par les éléments (w,x) pour lesquels le nombre de coordonnées non nulles de $x = (x_1,\dots,x_n)$ est pair.

4.5. Exercice (Version matricielle et présentation)

1. *Pour $w \in \mathfrak{S}_n$, on note P_w la matrice de permutation correspondante. Pour $x = (x_i) \in E$, on note P_x la matrice diagonale dont le i-ème coefficient diagonal est $(-1)^{x_i}$. Montrer qu'il existe un unique morphisme $\rho : B_n \to \mathrm{O}_n(\mathbb{R})$ injectif qui envoie $w \in \mathfrak{S}_n$ sur P_w et $x \in E$ sur P_x.*
2. *Montrer que B_n est engendré par les transpositions simples $s_i = (i, i+1)$ $(1 \leqslant i \leqslant n-1)$ et $t = (1,0,\dots,0) \in E$. Vérifier les relations suivantes*

[5] La distance de Hamming de deux vecteurs est le nombre de coordonnées distinctes.

(où e est le neutre de B_n) :

$$\begin{cases} t^2 = s_i^2 = e & (1 \leqslant i \leqslant n-1) \\ (s_i s_{i+1})^3 = e & (1 \leqslant i \leqslant n-2) \\ (s_i s_j)^2 = e & (1 \leqslant i, j \leqslant n-1,\ |i-j| \geqslant 2) \\ (s_1 t)^4 = e = (s_i t)^2 & (2 \leqslant i \leqslant n-1). \end{cases}$$

Ces relations sont en fait une présentation de B_n, voir [10].

3. *Montrer que D_n est engendré par les transpositions simples $s_i = (i, i+1)$ $(1 \leqslant i \leqslant n-1)$ et $u = (1, 1, \ldots, 0)$. Vérifier les relations :*

$$(s_2 u)^3 = e = (s_i u)^2 \ \big(i \in \{1, 3, 4, \ldots, n-1\}\big).$$

Avec les relations précédentes pour les s_i, c'est une présentation de D_n.

4.6. Proposition. *Pour n entier non nul, le groupe des symétries de la configuration de Clifford-Möbius d'ordre n est le groupe D_n.*

Démonstration. Le groupe $\mathfrak{S}_n$ agit linéairement sur $E = (\mathbb{Z}/2\mathbb{Z})^n$ par permutation des coordonnées et E agit sur lui-même par translations donc $B_n \simeq \mathfrak{S}_n \ltimes E$ agit comme un sous-groupe du groupe affine de E. Cette action préserve la somme de deux vecteurs de E : en effet, c'est évident pour une permutation et pour la translation de vecteur v, on a pour deux parties I et J : $e_I + v + e_J + v = e_I + e_J$. Autrement dit, l'action préserve la différence symétrique sur les parties. De plus, le sous-groupe D_n envoie une partie sur une partie dont le cardinal a la même parité. Ces deux faits permettent de dire que D_n s'injecte dans le groupe de symétries de la configuration. (Bien sûr, cette action est libre car D_n est un sous-groupe du groupe affine de E, lequel agit librement sur E.)

Soit G le groupe des automorphismes de la configuration, montrons que le quotient G/D_n est trivial. Soit g un élément de G, on va montrer que $gD_n = D_n$. Quitte à composer par une translation de E, ce qui ne change pas la classe gD_n, on peut supposer que g fixe $A_\emptyset$. Mais alors, g stabilise les cercles qui contiennent $A_\emptyset$, à savoir les cercles C_i $(i \in \{1, \ldots, n\})$. Quitte à composer par un élément de $\mathfrak{S}_n$, on peut supposer que g fixe chacun de ces cercles. Mais les points et les cercles associés à une partie I avec $|I| \geqslant 2$ sont parfaitement déterminés par ceux associés aux parties de cardinal strictement plus petit que $|I|$. Ainsi, une récurrence sur le cardinal de la partie montre que g est l'identité, si bien que le quotient G/D_n est trivial.□

4.7. Remarque. Un élément de $B_n \setminus D_n$ change la parité du cardinal des parties mais préserve la différence symétrique. Autrement dit, il échange points et lignes de la configuration, ce qui montre qu'elle est auto-duale.

4.8. Remarque. Par [H2G2, corollaire XI-3.4.5], on sait faire agir le groupe $\mathrm{PGL}_2(\mathbb{C})$ par homographies sur l'ensemble des cercles de la sphère de Riemann. On pourrait espérer un instant réaliser les automorphismes de la configuration par ces homographies. Mais c'est impossible. D'une part, la liste des sous-groupes finis de $\mathrm{PSL}_2(\mathbb{C})$ est connue et ni D_n, ni B_n n'y figure —sauf si $n \leqslant 2$ (voir le chapitre XI). D'autre part, des raisons de dimension empêchent qu'il n'y ait qu'une seule orbite de configurations de Clifford sous $\mathrm{PSL}_2(\mathbb{C})$: une configuration est déterminée par les $2(n+1)$ coordonnées réelles de $A_\emptyset$ et des centres des C_i alors que $\mathrm{PSL}_2(\mathbb{C})$ est de dimension réelle 6.

4.9. Remarque. Il est amusant de constater que le théorème de Miquel-Clifford résulte de considérations sur un cube (la formule des six birapports) et que la configuration finale soit (une réalisation d')un hypercube avec le groupe de symétries afférent.

Références : Nous devons à Christoph Soland la référence [19] et la notation uniforme des points et des droites par des fonctions indicatrices, qui rend évidents le lien avec l'hypercube et le groupe de symétries de la configuration pour un nombre quelconque de cercles initiaux.

Donald Coxeter présente la « chaîne de Clifford » dans [19] et le « groupe de symétries et réciprocités » de la configuration dans le §11 de [18]. On retrouve dans le livre [68] la configuration et son groupe de symétries (§5.3.7) ainsi que d'autres réalisations géométriques (§6.3.2) ; le lien avec la chaîne de Clifford est fait par Gábor Gévay et Tomaž Pisanski dans [36, §4].

5. Coloriages

Le but de cette partie est d'introduire la notion de combinatoire G-équivariante. Ici, on colorie un ensemble fini X de cardinal n sur lequel un groupe G agit et on veut compter le nombre de coloriages possibles modulo l'action de G.

Colorier X, c'est assigner à chaque élément de X une couleur, c'est-à-dire un élément d'un ensemble K de couleurs. Un *coloriage* de X est donc par définition une application de X vers K. Si K est fini de cardinal k, le nombre de coloriages est bien connu : c'est $N = k^n$. Il est utile de déformer ce nombre en un polynôme $P = (\sum_{i \in K} X_i)^n \in \mathbb{Q}[X_1, \ldots, X_k]$. Il s'agit bien d'une déformation dans le sens que si l'on évalue P en $(1, \ldots, 1)$, on retrouve N. Pourquoi étudier cette déformation ? Tout simplement parce que les coefficients vont nous donner des nombres intéressants : le coefficient en $\prod_i X_i^{n_i}$ de P, qui est égal bien entendu au nombre multinomial $\binom{n}{n_1,\ldots,n_k}$, n'est rien d'autre que le coloriage de X avec n_i

éléments de couleur i pour tout i. On reconnaît ici le lien fondamental entre combinatoire et polynômes symétriques (voire séries formelles symétriques), si fécond depuis Pascal et Newton.

Les questions que l'on se posera ici sont légitimes : si un groupe fini G agit sur X, alors G agit de façon naturelle sur les coloriages de X.

5.1. Question. Combien y a-t-il de coloriages modulo action de G ?

5.2. Question. Combien y a-t-il de coloriages, modulo action de G, possédant un nombre prédéfini de couleurs ?

Pour répondre à ces questions, avec K fixé, nous allons associer à l'action de G sur X un polynôme symétrique P de $\mathbb{Q}[X_1, \ldots, X_k]^{\mathfrak{S}_k}$ dont les coefficients y répondront de façon explicite et dont le calcul est donné par le théorème de Pólya.

Nous discuterons ensuite des applications d'une telle construction. Il s'agit encore là d'un joli thème qui mèle avec bonheur combinatoire, action de groupes, géométrie, polynômes symétriques/séries formelles, et même théorie des représentations, voir la proposition 5.36.

Il est conseillé de se munir d'un tétraèdre (sans oublier son groupe d'isométries positives $\mathfrak{A}_4$), voire d'un octaèdre (en billets de dix euros) et de crayons de couleurs afin d'aborder le sujet.

5.3. Théorème de Burnside pondéré et polynôme des coloriages

Soit X un ensemble de cardinal n sur lequel un groupe fini G agit. Pour un ensemble de couleurs $K = \{1, \ldots, k\}$, on associe l'ensemble de coloriages $\mathscr{C} = K^X$ des applications de X dans K. On peut construire deux actions sur $\mathscr{C}$: l'action (à droite) de G définie par

$$g \cdot f(x) = f(g \cdot x), \quad (g \in G,\ x \in X,\ f \in \mathscr{C})$$

et l'action (à gauche) du groupe $\mathfrak{S}(K)$ de permutations de X définie par

$$\sigma \cdot f(x) = \sigma\big(f(x)\big), \quad (\sigma \in \mathfrak{S}(K),\ x \in X,\ f \in \mathscr{C}).$$

Ces deux actions commutent.

Pour tout f de $\mathscr{C}$, on définit le monôme

$$\gamma(f) = \prod_{i=1}^{k} X_i^{n_i}, \quad \text{où } \forall i,\ n_i = f^{-1}(i) = \big|\{x \in X,\ f(x) = i\}\big|.$$

Pour tout g de G la bijection $x \mapsto g \cdot x$ de X établit une correspondance bijective entre $\{x \in X,\ f(x) = i\}$ et $\{x' \in X,\ f(g^{-1} \cdot x') = i\}$. Il en résulte que $\gamma(g \cdot f) = \gamma(f)$ et donc que γ passe au quotient en une application $\bar{\gamma}$ du quotient $\mathscr{C}/G$ dans $\mathbb{Q}[X_1, \ldots, X_k]$. Cela donne un sens à la définition suivante.

5.4. Définition. On définit le *polynôme générateur* P des coloriages G-invariants sur X par les couleurs K :

$$P = \sum_{\bar{f} \in \mathscr{C}/G} \bar{\gamma}(\bar{f}) \in \mathbb{Q}[X_1, \ldots, X_k].$$

5.5. Exercice. *Montrer que l'action du groupe $\mathfrak{S}(K)$ sur $\mathscr{C}$ passe au quotient en une action de $\mathfrak{S}(K)$ sur $\mathscr{C}/G$ et en déduire que le polynôme P est un polynôme symétrique de $\mathbb{Q}[X_1, \ldots, X_k]$.*

Pour $\sigma \in \mathfrak{S}(K)$, et $f \in \mathscr{C}$, on définit $\sigma \cdot f(x) = \sigma\big(f(x)\big)$. On définit une action qui commute à l'action de G et donc, qui passe à une action de $\mathfrak{S}(K)$ sur $\mathscr{C}/G$. On vérifie ensuite que $\sigma \cdot \big(\gamma(\bar{f})\big) = \gamma\big(\sigma \cdot (\bar{f})\big)$.

5.6. Exemple. Prenons comme exemple le coloriage des faces du tétraèdre régulier. Par [H2G2, proposition XII-3.12], le groupe G des isométries positives du tétraèdre est isomorphe à $\mathfrak{A}_4$ et donc G agit sur l'ensemble de ses faces et donc sur l'ensemble de ses coloriages par $K = \{1, 2\}$. On pourra imaginer que 1 est la couleur rouge et 2 le bleu.

On se convainc facilement, un tétraèdre à la main (ou dans la tête), qu'il y a, à isométrie près, cinq coloriages possibles : deux unicolores, deux bicolores avec trois faces d'une couleur et une de l'autre et enfin un coloriage bicolore avec deux faces de chaque couleur.

Le polynôme P est donc : $P = X_1^4 + X_1^3 X_2 + X_1^2 X_2^2 + X_1 X_2^3 + X_2^4$.

Pour calculer P, on le relie à un polynôme Q de l'algèbre $\mathbb{Q}[Y_1, \ldots, Y_n]$ où $n = |X|$.

5.7. Définition. Pour g dans G, soit Q_g le monôme $Q_g = \prod_{j=1}^{n} Y_j^{m_j(g)}$, où $m_j(g)$ est le nombre d'orbites de cardinal j pour l'action du groupe $\langle g \rangle$ engendré par g sur l'ensemble X.

On définit le *polynôme indicateur des cycles* pour l'action de G sur X par :

$$Q = \frac{1}{|G|} \sum_{g \in G} Q_g = \frac{1}{|G|} \sum_{g \in G} \prod_{j=1}^{n} Y_j^{m_j(g)} \in \mathbb{Q}[Y_1, \ldots, Y_n].$$

Le polynôme Q est *a priori* plus facile à calculer que le polynôme P puisqu'il provient directement de l'action de G sur X, alors que P provient de l'action de G sur $\mathscr{C}$.

5.8. Remarque. Si l'on note $\psi : G \to \mathfrak{S}(X)$ l'action de G sur X, alors $G/\ker\psi$ agit sur X par passage au quotient et l'on ne change pas le polynôme indicateur de cycle en remplaçant l'action de G par celle de $G/\ker\psi$.

On vérifie facilement cette propriété en regroupant dans la somme les éléments g d'une même classe modulo le noyau de l'action. On pourra donc se ramener à l'image de G par ψ. Dit autrement, le calcul du polynôme indicateur de cycles se ramène au cas où G est un sous-groupe de $\mathfrak{S}(X)$ agissant naturellement sur X.

5.9. Exemple. Pour l'action de $\mathfrak{S}_3$ sur $\{1,2,3\}$, on a

$$Q = (Y_1^3 + 3Y_1Y_2 + 2Y_3)/6\,.$$

Dans l'exercice IV-A.13, nous avons déjà calculé $Q(X,\dots,X)$ pour l'action de $\mathfrak{S}_n$ sur $\{1,\dots,n\}$. Pour $n=3$, on a : $Q(X,X,X) = (X^3+3X^2+2X)/6$, qui se factorise en $X(X+1)(X+2)/6$. En revanche, Q est irréductible.

5.10. Remarque. On remarque que pour g et h dans le groupe G, l'application $x \mapsto h\cdot x$ induit une bijection entre l'ensemble des orbites de X sous $\langle g\rangle$ et celui des orbites de X sous $\langle hgh^{-1}\rangle$. Pour un calcul pratique du polynôme indicateur, on peut donc regrouper tous les éléments g d'une même classe de conjugaison C_g. Cela donne :

$$Q = \frac{1}{|G|}\sum_g |C_g| \prod_{j=1}^{n} Y_j^{m_j(g)} \in \mathbb{Q}[Y_1,\dots,Y_n],$$

où g parcourt un ensemble de représentants des classes de conjugaison de G.

5.11. Remarque. La remarque 5.8 nous engage à nous concentrer sur le cas où G est un sous-groupe de $\mathfrak{S}(X) \simeq \mathfrak{S}_n$ et la remarque 5.10 va nous permettre de préciser le calcul dans ce cas. En effet, $\mathfrak{S}_n$ est la réunion disjointe de ses classes de conjugaison C_λ, où λ parcourt l'ensemble des partitions de n, comme dans l'exercice X-C.10. On rappelle que C_λ est l'ensemble des permutations de $\mathfrak{S}_n$ dont la suite des longueurs dans la décomposition en cycles disjoints est la partition λ. Pour tout g dans G, $m_j(g)$ ne dépend que de la partition λ_g associée à la permutation g : si l'on note $m_j(\lambda)$ le nombre de cycles de longueur j dans la partition λ de n, on a : $m_j(g) = m_j(\lambda_g)$. On trouve alors :

$$Q = \frac{1}{|G|}\sum_{\lambda\vdash n} |C_\lambda \cap G| \prod_j Y_j^{m_j(\lambda)} \in \mathbb{Q}[Y_1,\dots,Y_n],$$

où, rappelons-le, $\lambda \vdash n$ signifie que λ est une partition de n.

5.12. Exemple. Nous allons calculer le polynôme Q pour notre tétraèdre. Rappelons que le groupe d'isométries positives G est constitué de l'élément neutre e, tel que $Q_e = Y_1^4$, de huit rotations d'ordre 3, telles que $Q_r = Y_1Y_3$ et enfin de 3 retournements tels que $Q_s = Y_2^2$. On trouve finalement $Q = Y_1^4/12 + 2Y_1Y_3/3 + Y_2^2/4$.

Le *théorème de Pólya* établit un lien entre P et Q grâce aux polynômes de Newton, une famille particulière de polynômes symétriques.

5.13. Définition. Soit k un entier non nul fixé. Pour s entier naturel non nul, on pose

$$p_s = X_1^s + \cdots + X_k^s.$$

et l'on convient que $p_0 = 1$. Pour $\lambda{=}(\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_r)$, une partition de poids $n = \sum_{i \geqslant 1} \lambda_i$, le *polynôme de Newton* p_λ associé à λ est :

$$p_\lambda = \prod_{i=1}^{r} p_{\lambda_i}.$$

Voici donc la solution au problème de la combinatoire des coloriages G-invariants.

5.14. Théorème (Pólya). *Soit G un groupe fini agissant sur un ensemble fini X de cardinal n et soit K un ensemble de couleurs de cardinal k. Alors, le polynôme générateur des coloriages P et l'indicateur des cycles Q sont reliés par :*

$$P = Q(p_1, \ldots, p_n) \in \mathbb{Q}[X_1, \ldots, X_k].$$

5.15. Remarque. Dans l'exercice 5.5, on a vu que P est un polynôme symétrique. On savait donc à l'avance que P s'écrit comme un polynôme à coefficients rationnels en fonction des polynômes de Newton. Le théorème fournit donc une expression raisonnable, en termes de calculs, pour ce polynôme.

5.16. Remarque. Il est facile de calculer les cas extrêmes, c'est-à-dire lorsque G est le groupe trivial et lorsque G est le groupe $\mathfrak{S}(X)$ agissant naturellement sur X. Dans le premier cas, on trouve $P = p_1^n$, comme l'introduction le laissait supposer. Dans le second cas, on obtient

$$P = \frac{1}{n!} \sum_{\lambda \vdash n} |C_\lambda| p_\lambda,$$

où C_λ est la classe de conjugaison des permutations associées à la partition λ, *i.e.* les permutations dont la taille des cycles dans la décomposition en cycles disjoints est $\lambda{=}(\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_r)$. Voir [65] pour le calcul de $|C_\lambda|$.

5.17. Exemple. Pour le tétraèdre colorié par deux couleurs, on a facilement :

$$\begin{aligned} P &= \frac{1}{12}(X_1+X_2)^4 + \frac{2}{3}(X_1+X_2)(X_1^3+X_2^3) + \frac{1}{4}(X_1^2+X_2^2)^2 \\ &= X_1^4 + X_1^3X_2 + X_1^2X_2^2 + X_1X_2^3 + X_2^4. \end{aligned}$$

Le théorème repose sur la *formule de Burnside pondérée*, variante de la classique formule de Burnside IX-1.10.

5.18. Lemme (Formule de Burnside pondérée). *Soit G un groupe fini agissant sur un ensemble fini Y et soit $\pi : Y \to Y/G$ l'application canonique. Soit $\bar{\varphi}$ une fonction de Y/G vers un $\mathbb{Q}$-espace vectoriel et*[6] *$\varphi = \bar{\varphi} \circ \pi$. Alors, on a l'égalité*

$$\sum_{\bar{y} \in Y/G} \bar{\varphi}(\bar{y}) = \frac{1}{|G|} \sum_{g \in G} \sum_{y \in Y^g} \varphi(y),$$

où, pour g dans G, on note Y^g l'ensemble des éléments de Y fixés par g.

5.19. Remarque. Avant d'attaquer la preuve du théorème, on notera que la formule porte bien son nom : lorsque $\bar{\varphi}$ est la fonction constante égale à 1 (à valeurs dans $\mathbb{Q}$), on retrouve bien la formule de Burnside classique IX-1.10.

Démonstration. Comme pour la formule classique IX-1.10, l'idée est de calculer de deux manières l'expression $e = \sum_{(g,y) \in R} \varphi(y)$, où $R = \{(g,y) \in G \times Y,\ g \cdot y = y\}$.

D'une part, en notant G_y le stabilisateur d'un élément y de Y pour l'action de G, cette expression s'écrit

$$e = \sum_{y \in Y} \sum_{g \in G_y} \varphi(y) = \sum_{y \in Y} |G_y| \varphi(y) = \sum_{o \in Y/G} \sum_{y \in o} \frac{|G|}{|o|} \bar{\varphi}(o) = |G| \sum_{o \in Y/G} \bar{\varphi}(o).$$

D'autre part, on a :

$$e = \sum_{g \in G} \sum_{y \in Y^g} \varphi(y). \qquad \square$$

Démonstration (du théorème). On applique ce lemme avec G agissant sur $Y = \mathscr{C}$ et $\bar{\varphi} = \bar{\gamma} : Y/G \to \mathbb{Q}[X_1, \ldots, X_k]$. On obtient :

$$P = \sum_{\bar{f} \in \mathscr{C}/G} \bar{\gamma}(\bar{f}) = \frac{1}{|G|} \sum_{g \in G} \sum_{f \in \mathscr{C}^g} \gamma(f).$$

Fixons g dans G et interprétons le terme $\sum_{f \in \mathscr{C}^g} \gamma(f)$. On voit que f est

[6] Autrement dit, φ est constante sur les G-orbites et passe au quotient en $\bar{\varphi}$.

invariante par g si et seulement si $f(g^{-1}\cdot x) = f(x)$ pour tout x de X, c'est-à-dire si elle est constante sur les orbites de $\langle g\rangle$ agissant sur X. Si l'on décompose X en une réunion disjointe $\bigcup_{s=1}^{t} X^s$ de t orbites pour $\langle g\rangle$, et que l'on fixe un représentant $x^s \in X^s$ dans chaque orbite, alors l'application $f \mapsto \big(f(x^s)\big)_{1\leqslant j\leqslant t}$ établit une bijection (bien définie !) de $\mathscr{C}^g$ vers K^t. On a donc, en notant $|X^s| = n_s$:

$$\sum_{f\in\mathscr{C}^g} \gamma(f) = \sum_{(k_1,\dots,k_t)\in K^t} \prod_{s=1}^{t} X_{k_s}^{n_s} = \prod_{s=1}^{t}\sum_{i=1}^{k} X_i^{n_s} = \prod_{s=1}^{t} p_{n_s}.$$

Cette dernière expression peut se récrire sous la forme $\prod_{o\in\mathscr{C}/\langle g\rangle} p_{|o|}$. Il ne reste plus qu'à conclure :

$$P = \frac{1}{|G|}\sum_{g\in G}\prod_{o\in\mathscr{C}/\langle g\rangle} p_{|o|} = \frac{1}{|G|}\sum_{g\in G}\prod_{j=1}^{n} p_j^{m_j(g)},$$

et l'on obtient donc la formule désirée. □

On peut trouver agréable de récrire le théorème sous la forme suivante. La preuve est immédiate, si l'on se réfère à la remarque 5.11.

5.20. Corollaire. *Soit G un sous-groupe de $\mathfrak{S}_n$ agissant naturellement sur l'ensemble $X = \{1,\dots,n\}$. Alors,*

$$P = \frac{1}{|G|}\sum_{\lambda\vdash n} |C_\lambda \cap G| p_\lambda.$$

En évaluant tous les X_i en 1, on obtient le nombre de coloriages possibles modulo G. On remarquera que l'on retrouve intrinsèquement le théorème de Burnside (non pondéré).

5.21. Corollaire. *Soit G un groupe agissant sur un ensemble X. Le nombre de coloriages de X avec k couleurs et modulo l'action de G est égal à*

$$\frac{1}{|G|}\sum_{g\in G} k^{|X/\langle g\rangle|}.$$

Voici qui répond déjà précisément à la question 5.1.

5.22. Cas où k est assez grand

Afin de répondre à la question 5.2, la formule relativement explicite du corollaire 5.20 peut être rendue plus précise. En effet, si l'on veut connaître le nombre de coloriages G-invariants possédant un nombre prédéfini de couleurs, il faut décomposer le polynôme P dans une autre base que celle des p_λ.

Par exemple, pour calculer le nombre de coloriages de notre tétraèdre avec une face rouge (rouge = 1) et trois bleues (bleu = 2), on cherche le coefficient de $X_1X_2^3$ dans P. Comme P est symétrique, c'est aussi le coefficient en le polynôme symétrique monomial $m_{3\geqslant 1} = X_1X_2^3 + X_1^3X_2$ associé à la partition $(3 \geqslant 1)$ de 4.

Plus généralement, on sait[7] que l'espace des polynômes symétriques à k variables qui sont homogènes de degré n possède une base appelée *base monomiale* indexée par les partitions μ de n, et définie par

$$m_\mu = \sum_{1\leqslant i_1,\dots,i_r\leqslant k} \prod_{j=1}^{r} X_{i_j}^{\mu_j} \quad \text{si } \mu = (\mu_1 \geqslant \mu_2 \geqslant \cdots \geqslant \mu_r),\ \sum_{i\geqslant 1} \mu_i = n.$$

Répondre à la question 5.2 revient à déterminer les coefficients de P dans cette base monomiale. Il suffit donc de connaître les coefficients de la base des polynômes de Newton $(p_\lambda)_{\lambda\vdash n}$ dans la base monomiale $(m_\mu)_{\mu\vdash n}$. Il se trouve que pour k assez grand, plus précisément pour $k \geqslant n$, ces coefficients ne dépendent pas de k.

5.23. Exemple. On suppose $n = 4$ et $\lambda = (2 \geqslant 1 \geqslant 1)$. On vérifie facilement que

- pour $k = 1$: $p_\lambda = m_4$,
- pour $k = 2$: $p_\lambda = m_4 + 2m_{3\geqslant 1} + 2m_{2\geqslant 2}$,
- pour $k = 3$: $p_\lambda = m_4 + 2m_{3\geqslant 1} + 2m_{2\geqslant 2} + 2m_{2\geqslant 1\geqslant 1}$,
- pour $k \geqslant 4$: $p_\lambda = m_4 + 2m_{3\geqslant 1} + 2m_{2\geqslant 2} + 2m_{2\geqslant 1\geqslant 1} + 0m_{1\geqslant 1\geqslant 1\geqslant 1}$.

On a le droit de penser que mettre deux lignes pour les cas $k = 3$ et $k \geqslant 4$ était inutile, vu que le dernier coefficient est nul. On a préféré insister pour suggérer que derrière cette décomposition se cache l'ordre de dégénérescence des partitions déjà rencontré dans [H2G2, définition III-B.3.1] en termes de tableaux de Young : les termes non nuls dans la décomposition correspondent à des partitions μ supérieures à λ.

Pour λ et μ partitions de n, soit $\alpha_{\lambda,\mu}$ le coefficient de p_λ dans la base $(m_\mu)_{\mu\vdash n}$:

$$\forall \lambda \vdash n, \quad p_\lambda = \sum_{\mu\vdash n} \alpha_{\lambda,\mu} m_\mu.$$

On suppose ici que le nombre k de couleurs est inférieur ou égal à n, de sorte que toute partition de n possède au plus k parts (termes non nuls). Cela implique que les $\alpha_{\lambda,\mu}$ ne dépendent pas de k. Ces constantes sont bien connues des combinatoriciens : voir [48, p. 103] ou l'exercice 5.25 pour une interprétation combinatoire de ces constantes.

Le corollaire 5.20 implique alors immédiatement le suivant.

[7] Et si on l'ignore, il est très facile de le vérifier.

5.24. Corollaire. *Soit G un sous-groupe de $\mathfrak{S}_n$ agissant naturellement sur l'ensemble $X = \{1, \ldots, n\}$ et soit μ une partition de n. Alors, le nombre de coloriages de X avec μ_1 éléments de couleur 1,..., μ_k éléments de couleur k, modulo l'action de G est égal au coefficient de m_μ dans P, c'est-à-dire*

$$\kappa_\mu = \frac{1}{|G|} \sum_{\lambda \vdash n} \alpha_{\lambda,\mu} |C_\lambda \cap G|.$$

5.25. Remarque. Il est connu que les partitions λ qui apparaissent dans la somme (*i.e.* $\alpha_{\lambda,\mu} \neq 0$) sont inférieures à μ pour l'ordre de dégénérescence.

5.26. Application aux solides platoniciens

Pour chaque solide platonicien, on considère le groupe d'isométries du solide agissant sur ses faces. On calcule le polynôme indicateur des cycles Q. Pour le cube, un coup d'œil sur l'objet suffira. Pour l'octaèdre, il suffira, par dualité (au sens de [H2G2, définition XII-4.1]), de regarder un cube et de considérer l'action du groupe du cube sur l'ensemble de ses sommets. Pour le dodécaèdre, on pourra se rapporter à [H2G2, §XII-3.6] et pour l'icosaèdre, on utilisera encore la dualité.

1. Le tétraèdre :
$$Q = \frac{1}{12}(Y_1^4 + 8Y_1Y_3 + 3Y_2^2).$$
Déjà vu en exercice.

2. Le cube :
$$Q = \frac{1}{24}(Y_1^6 + 6Y_1^2Y_4 + 3Y_1^2Y_2^2 + 6Y_2^3 + 8Y_3^2).$$
Dans l'ordre, les termes correspondent à l'identité, aux six quarts de tour autour des axes passant par les centres de deux faces opposées, aux trois demi-tours autour des axes passant par les centres de deux faces opposées, aux six demi-tours dont les axes passent par les milieux d'arêtes opposées et enfin aux huit rotations d'ordre 3 autour des grandes diagonales.

3. L'octaèdre :
$$Q = \frac{1}{24}(Y_1^8 + 8Y_1^2Y_3^2 + 9Y_2^4 + 6Y_4^2).$$
Ici encore, les termes correspondent dans l'ordre à l'identité, aux huit rotations d'ordre 3 autour des axes passant par les centres de deux faces opposées, aux trois demi-tours autour des axes passant par des sommets opposés et aux six demi-tours (3+6 = 9) dont les axes passent par les milieux d'arêtes opposées et enfin aux six quarts de tour dont les axes passent par deux sommets opposés.

4. Le dodécaèdre :
$$Q = \frac{1}{60}(Y_1^{12} + 24Y_1^2Y_5^2 + 15Y_2^6 + 20Y_3^4).$$
Les termes correspondent, dans l'ordre, à l'identité, aux vingt-quatre rotations d'ordre 5 autour des axes passant par les centres de faces opposées, aux quinze demi-tours passant par les milieux d'arêtes opposées, et enfin aux vingt rotations d'ordre 3 dont les axes passent par deux sommets opposés.
5. L'icosaèdre :
$$Q = \frac{1}{60}(Y_1^{20} + 20Y_1^2Y_3^6 + 15Y_2^{10} + 24Y_5^4).$$
Les termes correspondent à l'identité, aux vingt rotations d'ordre 3 dont les axes passent par les centres de deux faces opposées, aux quinze demi-tours dont les axes passent par le milieu d'arêtes opposées, et aux vingt-quatre rotations d'ordre 5 dont les axes passent par des sommets opposés.

5.27. Le collier de pierres

Le problème ici est de savoir combien de colliers différents on peut créer avec n pierres de k couleurs différentes. On peut considérer deux sous-problèmes selon que l'on considère que deux colliers sont identiques modulo rotation ou identiques modulo rotation et retournement. Dans le premier cas, il s'agit du problème de coloriage modulo l'action de $\mathbb{Z}/n\mathbb{Z}$ et dans le second cas, modulo l'action du groupe diédral D_n. Quitte à manquer de poésie dans ce beau problème qui a mis en scène Roméo et Juliette, ainsi que l'inoubliable Suleima, nous allons considérer le collier comme un polygone régulier à n sommets.

Premier cas : action de $\mathbb{Z}/n\mathbb{Z}$.

Pire encore, nous sommes amenés à considérer l'action de $\mathbb{Z}/n\mathbb{Z}$ sur lui-même par translation, et ce, en assimilant le collier de pierres à $\mathbb{Z}/n\mathbb{Z}$. Cela permet d'utiliser quelques propriétés connues du groupe cyclique.

Rappelons cette propriété remarquable et souvent très utile de $\mathbb{Z}/n\mathbb{Z}$. Pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d, nécessairement cyclique. Le lecteur en panne d'inspiration pour prouver ce résultat pourra réaliser $\mathbb{Z}/n\mathbb{Z}$ comme le groupe des racines primitives complexes de l'unité, pour considérer les racines d-ièmes de l'unité. Il existe donc $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ et, par acquit de conscience, on vérifie que le compte est bon par la formule $\sum_{d|n} \varphi(d) = n$.

Pour un élément g d'ordre d, les orbites de $\langle g \rangle \simeq \mathbb{Z}/d\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ sont les classes modulo $\langle g \rangle$. Il y en a n/d et elle sont toutes de cardinal d. Il vient donc :
$$Q = \frac{1}{n}\sum_{d|n} \varphi(d)\, Y_d^{n/d}.$$

Deuxième cas : action du groupe diédral D_n.

On pourrait ici considérer l'action de D_n sur son sous-groupe cyclique d'ordre n, d'indice 2 et donc distingué. Il est plus visuel de considérer l'action de D_n sur le polygone régulier à n sommets. On rappelle que le groupe diédral est constitué de n rotations (d'ordre d divisant n) et n symétries (d'ordre 2). On connaît déjà par l'étude précédente les orbites de $\langle g \rangle$ lorsque g est une rotation.

Si n est impair, alors les axes de symétries du polygone sont les axes qui relient un sommet et le milieu de l'arête opposée. Il y a donc une orbite singletonne (le sommet) et $(n-1)/2$ orbites à deux éléments.

Si n est pair, il y a deux types d'axes de symétries. Soit les axes qui joignent deux sommets opposés, soit les axes qui joignent les milieux des arêtes opposées. Dans le premier cas, on a deux orbites singletonnes (les deux sommets) et $(n-2)/2$ orbites à deux éléments. Dans le second cas, on a $n/2$ orbites à deux éléments.

Il est largement temps de conclure :

$$Q = \frac{1}{2n}\Big(\sum_{d|n} \varphi(d) Y_d^{n/d} + n Y_1 Y_2^{(n-1)/2}\Big) \qquad \text{si } n \text{ est impair ;}$$

$$Q = \frac{1}{2n}\Big(\sum_{d|n} \varphi(d) Y_d^{n/d} + \frac{n}{2} Y_1^2 Y_2^{(n-2)/2} + \frac{n}{2} Y_2^{n/2}\Big) \qquad \text{si } n \text{ est pair.}$$

Tous les problèmes que l'on s'est posés sur la combinatoire des colliers que l'on peut créer avec n pierres de k couleurs différentes trouvent réponse dans le polynôme : $P = Q(p_1, \ldots, p_n)$, où les p_i sont les polynômes de Newton à k variables.

5.28. Combinatoire des arbres enracinés à isomorphisme près

L'étude des arbres enracinés constitue un sujet vibrant d'actualité. Pourtant, il remonte à Arthur Cayley, qui les introduit en 1857 dans [15] dans le but de décrire la composition d'opérateurs différentiels. Ils constituent une structure de données fondamentale en informatique comme archétype de la récursivité[8], et que l'on retrouve même en analyse numérique dans l'algorithme de Runge-Kutta. Ici, nous étudierons ces arbres afin de sensibiliser le lecteur à l'utilisation des séries formelles dans la combinatoire invariante sous un groupe.

Un *arbre enraciné* est un graphe sans cycle dont on marque un sommet que l'on appelle *racine*. Chaque sommet du graphe est appelé *nœud*. Chaque

[8]Donald Knuth, auteur de l'ouvrage de référence sur l'algorithmique, considère d'ailleurs les arbres comme « la structure la plus fondamentale de toute l'informatique ».

nœud possède un unique *père* (comme l'arbre généalogique d'un protozoaire) et peut avoir plusieurs *fils*. Ceux qui en ont seront appelés *nœuds internes*.

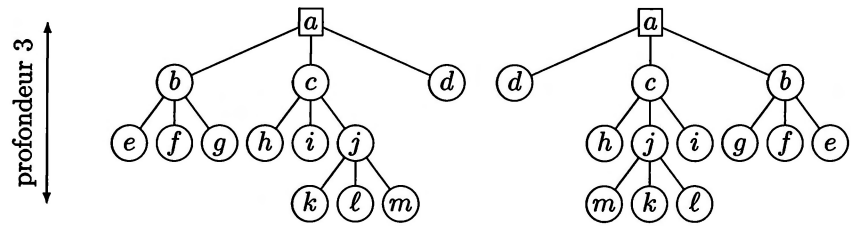


Figure 5.1. *Deux représentations du même arbre*

Nous allons nous intéresser, à titre d'exemple, aux arbres enracinés ternaires, ceux où tout nœud interne possède exactement trois fils. On voit que la construction de ces arbres peut se faire par récurrence sur le nombre de nœuds internes. En effet, un arbre à $m+1$ nœuds internes peut se contruire par *greffe* à l'aide d'une racine et de trois arbres ayant respectivement k_1, k_2 et k_3 nœuds internes, avec $k_1 + k_2 + k_3 = m$.

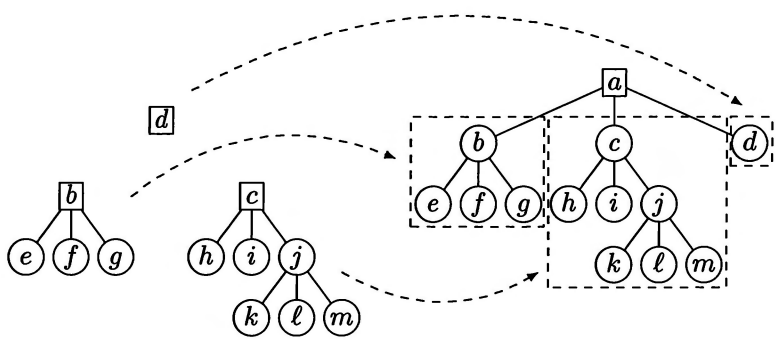


Figure 5.2. E pluribus unum

On trouvera naturel de considérer ces arbres modulo permutation des trois fils sortant de chaque nœud. On voit que la récurrence précédente permet aussi de construire ces arbres modulo permutation à la racine, puisque chaque nœud interne a été racine lors de la construction de l'arbre. Soit $\mathscr{T}$ l'ensemble des (classes d')arbres enracinés ternaires à isomorphisme près. Soit t_m le nombre d'arbres de $\mathscr{T}$ possédant exactement m nœuds internes.

5.29. Exercice. *Trouver toutes les classes d'arbres possédant au plus cinq nœuds internes. Constater que* $t_0 = t_1 = t_2 = 1$, $t_3 = 2$, $t_4 = 4$, $t_5 = 8$.

La *profondeur* d'un nœud est le nombre d'arêtes dans l'unique chemin qui le relie à la racine. On le calcule récursivement ainsi : la profondeur de la racine est 0 ; la profondeur d'un nœud est 1 de plus que celle de son père. La *profondeur*[9] d'un arbre est la profondeur maximale d'un de ses nœuds. Par exemple, dans la figure 5.2, les arbres dont les racines sont a, b, c et d ont pour profondeurs respectives 3, 1, 2 et 0. On note $\mathscr{T}_{\leqslant r}$ l'ensemble des (classes d')arbres enracinés ternaires de profondeur au plus r. Par exemple, $\mathscr{T}_{\leqslant 0}$ est constitué du seul arbre sans arête (racine seule). On note $t_{m,\leqslant r}$ le nombre d'arbres ternaires de profondeur au plus r ayant exactement m nœuds internes.

On introduit la série génératrice $S(T) = \sum_{m\geqslant 0} t_m T^m$ dans l'anneau $\mathbb{Q}[[T]]$ des séries formelles en T.

5.30. Lemme. *La série formelle S satisfait à la relation suivante :*

$$S(T) = 1 + \frac{T}{6}\big(S(T)^3 + 3S(T)S(T^2) + 2S(T^3)\big).$$

Autrement dit : $S = 1 + TQ\big(S(T), S(T^2), S(T^3)\big)$, où Q est le polynôme indicateur des cycles pour l'action naturelle de $\mathfrak{S}_3$ sur $X = \{1,2,3\}$, c'est-à-dire :

$$Q = \frac{1}{6}(Y_1^3 + 3Y_1Y_2 + 2Y_3).$$

Idée-clé. La construction récursive des arbres par greffe que nous venons de voir peut s'interpréter en termes de coloriages invariants. Soit r un entier naturel. Un arbre de profondeur au plus $r+1$ est déterminé par les trois sous-arbres attachés à la racine, qui sont un triplet d'éléments de $\mathscr{T}_{\leqslant r}$ à l'ordre près. Autrement dit, les éléments de $\mathscr{T}_{\leqslant r+1}$ sont en bijection avec les coloriages de $X = \{1,2,3\}$ par l'ensemble de couleurs $\mathscr{T}_{\leqslant r}$ modulo l'action de $\mathfrak{S}_3$.

Démonstration. On note d'une part que l'arbre de $\mathscr{T}_{\leqslant 0}$ (la racine seule) n'est pas obtenue par cette construction. D'autre part, si l'on note $\varpi(a)$ le nombre de nœuds internes d'un arbre a donné, et t l'arbre correspondant au coloriage γ tel que $\gamma(1) = a$, $\gamma(2) = b$, $\gamma(3) = c$, alors $\varpi(t) = 1 + \varpi(a) + \varpi(b) + \varpi(c)$. Soit $P_{\leqslant r}$ le *polynôme générateur*[10] des coloriages $\mathfrak{S}_3$-invariants sur X par les couleurs $\mathscr{T}_{\leqslant r}$. Alors, la construction par coloriage $t_{m,\leqslant r}$ est égal au coefficient de T^m dans le polynôme $1 + TP_{\leqslant r-1}(T^{\varpi(a)},\ a \in \mathscr{T}_{\leqslant r-1})$.

[9] Peut-être serait-il plus standard de parler de *hauteur*.

[10] C'est un polynôme en les variables X_a où a parcourt $\mathscr{T}_{\leqslant r}$. On le note $P(X_a, a \in \mathscr{T}_{\leqslant r})$.

En effet, le premier terme correspond à $\mathscr{T}_{\leqslant 0}$, la multiplication par T correspond au passage de $k-1$ à k nœuds internes dans la construction, et le comptage du nombre de nœuds internes pour une classe d'arbre a se fait en remplaçant la variable X_a associée par $T^{\varpi(a)}$. Autrement dit :

$$\sum_{m\geqslant 0} t_{m,\leqslant r} T^m = 1 + T\,P_{\leqslant r-1}\big(T^{\varpi(a)},\, a\in \mathscr{T}_{\leqslant r-1}\big).$$

En appliquant le théorème 5.14 et en sommant, on obtient :

$$\sum_{m\geqslant 0} t_{m,\leqslant r} T^m = 1 + TQ\Big(\sum_{a\in\mathscr{T}_{\leqslant r}} T^{\varpi(a)}, \sum_{a\in\mathscr{T}_{\leqslant r}} T^{2\varpi(a)}, \sum_{a\in\mathscr{T}_{\leqslant r}} T^{3\varpi(a)}\Big).$$

Comme les classes d'arbres à m nœuds internes peuvent être obtenus par cette construction, on a pour r assez grand (et m fixé) : $t_{m,\leqslant r} = t_m$. Pour être plus précis, disons qu'un arbre de profondeur r possède au moins r nœuds internes, et ainsi, $t_{m,\leqslant r} = t_m$ dès que $r \geqslant m$.

Il vient donc, en remarquant que $S(T) = \sum_{a\in\mathscr{T}} T^{\varpi(a)}$:

$$\begin{aligned} S(T) &= 1 + TQ\Big(\sum_{a\in\mathscr{T}} T^{\varpi(a)}, \sum_{a\in\mathscr{T}} T^{2\varpi(a)}, \sum_{a\in\mathscr{T}} T^{3\varpi(a)}\Big) \\ &= 1 + TQ\big(S(T), S(T^2), S(T^3)\big). \end{aligned}$$

On obtient alors la formule de récurrence suivante.

5.31. Proposition. *Pour tout entier m, on a :*

$$t_{m+1} = \frac{1}{6}\Big(\sum_{i+j+k=m} t_i t_j t_k + 3\sum_{i+2j=m} t_i t_j + 2\sum_{3i=m} t_i\Big),$$

où les indices i, j, k parcourent $\mathbb{N}$.

5.32. Exercice. *Retrouver par la proposition les résultats de l'exercice 5.29.*

On laisse le soin au lecteur de montrer que ce résultat se généralise pour des n-arbres et que l'on a dans ce contexte :

$$t_{m+1} = \frac{1}{n!}\Big(\sum_{\lambda\vdash n} |C_\lambda| \sum_{\sum_i \lambda_i a_i = m} \prod_i t_{a_i}\Big).$$

Les espaces projectifs finis donnent des exemples de graphes possédant une riche symétrie. On va donner deux exemples de coloriages des points d'un espace projectif fini, invariants pour l'action du groupe projectif correspondant.

5.33. Polynôme indicateur de cycles pour l'action de $\mathrm{PGL}_2(\mathbb{F}_q)$ sur $\mathbb{P}^1(\mathbb{F}_q)$

Soient p un nombre premier impair et q une puissance de p. On veut calculer le polynôme Q pour l'action de $\mathrm{PGL}_2(\mathbb{F}_q)$ sur la droite projective $\mathbb{P}^1(\mathbb{F}_q)$.

Au vu de la remarque 5.10, on se doit de calculer tout d'abord les classes de conjugaison du groupe $\mathrm{PGL}_2(\mathbb{F}_q)$. C'est fait dans la proposition B.9.

Étudions les cycles de $\mathrm{PGL}_2(\mathbb{F}_q)$ sur $\mathbb{P}^1(\mathbb{F}_q)$ au cas par cas. On va noter $[A]$ la classe d'une matrice inversible A dans le groupe projectif (notation réminiscente des coordonnées projectives $[x : y : z]$).

1. L'identité. Toute droite de $\mathbb{F}_q^2$ est stable par l'identité. Donc, tout point de $\mathbb{P}^1(\mathbb{F}_q)$ l'est. Il y a $q+1$ orbites à un élément.

2. Soit A dans $\mathrm{GL}_2(\mathbb{F}_q)$ diagonalisable à valeurs propres distinctes. On a deux (et seulement deux droites) stables par A. Elles sont stables par toute puissance A^k de A. Or, une puissance A^k possède une troisième droite stable si et seulement si A^k est une homothétie, c'est-à-dire si $[A]^k$ est le neutre de $\mathrm{PGL}_2(\mathbb{F}_q)$. Notons donc d l'ordre de $[A]$. On a vu que l'action du groupe cyclique engendré par A sur $\mathbb{P}^1(\mathbb{F}_q)$ possède 2 orbites à un élément et $(q-1)/d$ orbites à d éléments.

3. Soit A dans $\mathrm{GL}_2(\mathbb{F}_q)$ trigonalisable mais non diagonalisable. On a une (et seulement une) droite stable par A. Elle est stable par toute puissance A^k de A. Or, le spectre d'une puissance A^k étant une valeur propre double, A^k posséde une autre droite stable si et seulement si A^k est une homothétie, c'est-à-dire que $[A]^k$ est le neutre de $\mathrm{PGL}_2(\mathbb{F}_q)$. L'ordre de $[A]$ est p d'après le tableau de la proposition B.9. On conclut comme ci-dessus : l'action du groupe cyclique engendré par A sur $\mathbb{P}^1(\mathbb{F}_q)$ possède 1 orbite à 1 élément et q/p orbites à p éléments.

4. Soit A dans $\mathrm{GL}_2(\mathbb{F}_q)$ non trigonalisable. Aucune droite n'est stable par A. Les deux valeurs propres de toute puissance A^k de A sont dans $\mathbb{F}_{q^2}$, conjuguées par le Frobenius $z \mapsto z^q$, et si une telle puissance possédait une droite stable (dans $\mathbb{F}_q^2$), ses deux valeurs propres seraient alors dans $\mathbb{F}_q$ et égales. Ainsi, A^k serait une homothétie ou serait trigonalisable non diagonalisable.

   Montrons que ce dernier cas est impossible : on a dans le tableau de la proposition B.9 la relation $[A^k]^{q+1} = [\mathrm{I}_2]$, or si A^k était seulement trigonalisable, on aurait $[A^k]^p = [\mathrm{I}_2]$ et les deux équations donneraient $[A^k] = [\mathrm{I}_2]$, absurde. Soit d l'ordre de $[A]$, l'action du groupe cyclique engendré par A sur $\mathbb{P}^1(\mathbb{F}_q)$ possède donc $(q+1)/d$ orbites à d éléments.

On termine par un bilan des données du tableau de la proposition B.9. On obtient le polynôme indicateur des cycles pour l'action de $\mathrm{PGL}_2(\mathbb{F}_q)$ sur $\mathbb{P}^1(\mathbb{F}_q)$:

$$Q = \frac{1}{q(q-1)(q+1)} Y_1^{q+1} + \frac{1}{2(q-1)} \sum_{\substack{d \mid (q-1) \\ d>1}} \varphi(d) Y_1^2 Y_d^{(q-1)/d} + \frac{1}{q} Y_1 Y_p^{q/p} + \frac{1}{2(q+1)} \sum_{\substack{d \mid (q+1) \\ d>1}} \varphi(d) Y_1^2 Y_d^{(q+1)/d}.$$

Polynôme indicateur de cycles pour l'action de $\mathrm{PGL}_3(\mathbb{F}_2)$ sur le plan de Fano $\mathbb{P}^2(\mathbb{F}_2)$

Le groupe $\mathrm{PGL}_3(\mathbb{F}_2)$ a vocation d'agir sur le *plan de Fano*, qui, par définition, est le plan projectif $\mathbb{P}^2(\mathbb{F}_2)$, voir figure 5.3. L'intérêt ici est de colorier un graphe comportant, malgré son apparente simplicité, un riche groupe d'automorphismes et qui, pour ne rien gâter, se trouve être un groupe simple[11].

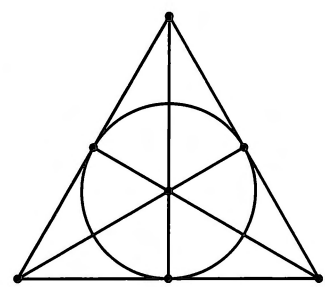


Figure 5.3. *Plan de Fano*

Pour étudier les classes de conjugaison de $\mathrm{PGL}_3(\mathbb{F}_2)$, nous allons utiliser l'isomorphisme exceptionnel $\mathrm{PGL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ établi plus loin (corollaire VII-4.2), et bien entendu la géométrie du plan de Fano.

Par la proposition B.12, on sait que les classes de conjugaison de $\mathrm{PSL}_2(\mathbb{F}_7)$, et donc de $\mathrm{PGL}_3(\mathbb{F}_2)$, se répartissent ainsi :

nombre de classes	1	1	2	1	1
ordre des éléments	1	3	7	2	4
cardinal de la (des) classe(s)	1	56	24	21	42

Grâce aux ordres, on va reconnaître les classes de conjugaison dans $\mathrm{PGL}_3(\mathbb{F}_2)$.

Nous allons répartir les classes de similitude de $\mathrm{GL}_3(\mathbb{F}_2)$ grâce aux invariants de similitude. On sait tout d'abord[12] que les polynômes irréductibles sur $\mathbb{F}_2$ de degré inférieur à 3 sont $X+1$, X^2+X+1, X^3+X+1, X^3+X^2+1. Les invariants de similitude possibles étant des polynômes qui se divisent successivement, et le produit de ceux-ci étant le polynôme caractéristique

[11] On pourra voir une application du coloriage du plan de Fano au jeu *Dobble* dans [12]. Un peu de culture mondaine à moindre frais, qui a permis aux auteurs de briller plus d'une fois en société.

[12] Et si l'on sait pas, c'est immédiat de le retrouver, car un polynôme de degré 2 ou 3 est irréductible sur un corps $\mathbb{K}$ si et seulement s'il n'a pas de racine dans $\mathbb{K}$.

(donc de degré 3) de la matrice, les seules possibilités sont :

$$\begin{array}{lll} ((X+1),(X+1),(X+1)), & ((X^2+X+1)(X-1)), & (X^3+X+1), \\ (X^3+X^2+1), & ((X+1)^2,(X+1)), & ((X+1)^3). \end{array}$$

Il y a donc six classes de conjugaison : le compte est bon. Rien d'étonnant en fait, mais ça restera toujours un plaisir. Affinons la correspondance à l'aide des ordres et en considérant les décompositions dans $\mathbb{F}_2[X]$:

$$\begin{array}{ll} X^2+1=(X+1)^2, & X^3+1=(X+1)(X^2+X+1), \\ X^4+1=(X+1)(X+1)^3, & (X+1)^7=(X+1)(X^3+X+1)(X^3+X^2+1). \end{array}$$

Comme le polynôme minimal de la classe de conjugaison est le premier invariant de similitude, les classes de conjugaison de $\mathrm{GL}_3(\mathbb{F}_2)$ ci-dessus ont pour ordres respectifs 1, 3, 7, 7, 2 et 4.

Le tableau suivant donne le résumé des classes de conjugaison de $\mathrm{GL}_3(\mathbb{F}_2)$.

invariants de similitude	card. classe	forme normale	ordre
$((X-1),(X-1),(X-1))$	1	$\begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}$	1
$((X^2+X+1)(X-1))$	56	$\begin{pmatrix} 1&0&0 \\ 0&0&1 \\ 0&1&1 \end{pmatrix}$	3
(X^3+X+1)	24	$\begin{pmatrix} 0&0&1 \\ 1&0&1 \\ 0&1&0 \end{pmatrix}$	7
(X^3+X^2+1)	24	$\begin{pmatrix} 0&0&1 \\ 1&0&0 \\ 0&1&1 \end{pmatrix}$	7
$((X-1)^2,(X-1))$	21	$\begin{pmatrix} 1&1&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}$	2
$((X-1)^3)$	42	$\begin{pmatrix} 1&1&0 \\ 0&1&1 \\ 0&0&1 \end{pmatrix}$	4

Figure 5.4. *Classes de conjugaison dans* $\mathrm{GL}_3(\mathbb{F}_2)$

On peut calculer le polynôme d'indicateur de cycles pour l'action du groupe $\mathrm{PGL}_3(\mathbb{F}_2)$ sur le plan de Fano :

$$Q = \frac{1}{168}(Y_1^7 + 56Y_1Y_3^2 + 48Y_7 + 21Y_1^3Y_2^2 + 42Y_1Y_2Y_4).$$

Le premier terme correspond à l'identité. Pour le deuxième, on voit que $\left(\begin{smallmatrix}1&0&0\\0&0&1\\0&1&1\end{smallmatrix}\right)$ possède une unique droite invariante et comme elle est d'ordre 3, les six droites restantes se répartissent en deux orbites de cardinal 3. Pour le troisième terme, les deux matrices $\left(\begin{smallmatrix}0&0&1\\1&0&1\\0&1&0\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}0&0&1\\0&1&0\\0&1&1\end{smallmatrix}\right)$ sont d'ordre 7 et n'ont pas de droite invariante. Pour la quatrième, on constate que $\left(\begin{smallmatrix}1&1&0\\0&1&0\\0&0&1\end{smallmatrix}\right)$, qui est d'ordre 2, possède un seul sous-espace propre et que celui-ci est de dimension 2 : elle possède donc exactement trois droites invariantes et les quatre droites restantes se répartissent en deux orbites de cardinal 2. Enfin, pour le dernier terme, on sait que la matrice $\left(\begin{smallmatrix}1&1&0\\0&1&1\\0&0&1\end{smallmatrix}\right)$, d'ordre 4, possède une unique droite invariante, et les six droites restantes ne peuvent que se répartir en une orbite de cardinal 2 plus une de cardinal 4.

Nous nous servirons de ce résultat dans l'exercice XI-C.14 pour le calcul de la table des caractères du groupe $\mathrm{GL}_3(\mathbb{F}_2)$.

5.34. Exercice. *Décrire géométriquement les orbites pour l'action du sous-groupe d'ordre* 4 *engendré par* $\left(\begin{smallmatrix}1&1&0\\0&1&1\\0&0&1\end{smallmatrix}\right)$ *sur le plan de Fano.*

5.35. Théorème de Pólya et représentation induite

Quitte à prendre un peu d'avance sur le chapitre X où nous introduirons, à titre informatif[13], quelques éléments de théorie des représentations, nous allons exprimer ici le théorème de Pólya en termes de caractères de représentations de groupes.

Toutes ces notions étant développées ultérieurement, nous nous contenterons ici de dire que si G est un groupe et V un espace vectoriel sur un corps $\mathbb{K}$, un morphisme ρ de G dans le groupe $\mathrm{GL}(V)$ est appelé *représentation* de G. Si (V,ρ) est une représentation de G, alors le caractère de la représentation est l'application χ_ρ de G dans $\mathbb{K}$ qui à g dans G associe la trace de $\rho(g)$. Par invariance de la trace, et comme ρ est un morphisme, il en résulte que χ_ρ est constant sur les classes de conjugaison de G.

On considère donc un ensemble X de cardinal n et un groupe G agissant sur X. On veut étudier les coloriages G-équivariants sur l'ensemble X et donc calculer le polynôme générateur P des coloriages pour cette action. Quitte à quotienter par le noyau de l'action, on peut se ramener au cas où l'action est fidèle et donc au cas où G est un sous-groupe de $\mathfrak{S}(X) \simeq \mathfrak{S}_n$.

Rappelons que pour toute partition $\lambda = (\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_r)$ de n, on a défini les polynômes symétriques p_λ, cf. 5.13 et la classe de conjugaison C_λ constituée de permutations dont la décomposition en cycles est associée à λ. On définit également l'ordre z_λ du stabilisateur pour l'action de $\mathfrak{S}_n$ par conjugaison d'un élément de C_λ, qui ne dépend pas de l'élément choisi.

[13] Ceci est une litote.

5.36. Proposition. *Soit G un groupe agissant fidèlement sur un ensemble X de cardinal n. Il existe une représentation (V,ρ) sur le corps $\mathbb{Q}$ du groupe $\mathfrak{S}_n$ telle que le polynôme générateur des coloriages pour l'action de G sur X est donné par*

$$P = \sum_{\lambda \vdash n} \frac{\chi_\rho(\lambda)}{z_\lambda} p_\lambda.$$

Si l'on fixe une injection de G dans $\mathfrak{S}_n$, alors la représentation (V,ρ) est la représentation induite *de la représentation triviale de G sur $\mathfrak{S}_n$, voir les exercices XI-C.4 à XI-C.6.*

Cette formule sera montrée dans l'exercice XI-C.7. Nous nous contenterons pour l'instant de faire une remarque sur la pertinence de cette interaction entre théorie de Pólya et théorie des représentations, voir [79].

5.37. Remarque. Nous verrons avec le théorème de Maschke X-A.12 que toute représentation (V,ρ) d'un groupe G se décompose en somme directe de représentations dites irréductibles : $V = \bigoplus_i V_i$, où les (V_i,ρ_i) sont des représentations telles qu'il n'existe pas de sous-espace de V_i non trivial stable par $\rho_i(G)$. En particulier, le caractère χ_ρ peut s'écrire $\chi_\rho = \sum_i a_i \chi_{\rho_i}$, où les a_i sont des entiers positifs. Cette positivité est une des justifications les plus légitimes de l'incursion de la théorie des représentations en combinatoire.

Les classes d'isomorphisme de représentations irréductibles de $\mathfrak{S}_n$ sur le corps $\mathbb{C}$ des complexes sont indexées par les partitions de n, ce qui est justifié par le fait que les classes de conjugaison de $\mathfrak{S}_n$ sont indexées par ces mêmes partitions, voir l'exercice X-C.10. Soit χ_μ le caractère associé à la partition μ de n et soit χ_ρ le caractère de l'induit introduit dans la proposition précédente. Nous avons alors : $\chi_\rho = \sum_\mu a_\mu \chi_\mu$ pour tout $a_\mu \in \mathbb{N}$, et donc

$$P = \sum_{\lambda \vdash n} \frac{1}{z_\lambda} p_\lambda \sum_{\mu \vdash n} a_\mu \chi_\mu(\lambda) = \sum_{\mu \vdash n} a_\mu s_\mu,$$

où l'on a posé

$$s_\mu = \sum_{\lambda \vdash n} \frac{\chi_\mu(\lambda)}{z_\lambda} p_\lambda.$$

Les polynômes symétriques s_μ sont appelés *fonctions de Schur*. Ils forment une base de l'algèbre des polynômes symétriques. Outre leurs propriétés combinatoires remarquables, ils jouent un rôle central dans la théorie des représentations des groupes symétriques et des groupes linéaires. Voir par exemple [31], [51], [48] ou [29].

Ici, on a montré par la théorie des représentations, que les polynômes générateurs des coloriages, qui sont des polynômes *a priori* symétriques, se décomposent dans la base des polynômes de Schur avec des coefficients entiers positifs. Cela n'était pas clair sans la théorie des représentations.

A. Annexe. Tangentes à une conique

Les notations suivantes seront utilisées dans toute l'annexe A.

A.1. Notations. Comme toujours pour parler de coniques, on se place sur un corps $\mathbb{K}$ de caractéristique différente de 2. Soit Q une forme quadratique non dégénérée sur $\mathbb{K}^3$. On note $\mathscr{N}_0$ le cône isotrope de Q et Φ la forme bilinéaire associée. Comme Q est homogène, $\mathscr{N}_0$ est une réunion de droites : on note $\mathscr{C}_0$ l'ensemble correspondant dans le plan projectif $\mathbb{P}^2(\mathbb{K}) = \mathbb{P}(\mathbb{K}^3)$: c'est l'image de $\mathscr{N}_0$ par la projection naturelle $\mathbb{K}^3 \setminus \{0\} \to \mathbb{P}(\mathbb{K}^3)$.

A.2. Description algébrique des tangentes

Supposons provisoirement que $\mathbb{K} = \mathbb{R}$. Étant donné un point p de $\mathscr{N}_0$ autre que l'origine et un vecteur $h \in \mathbb{K}^3$, on a : $Q(p+h) = Q(p) + 2\Phi(p,h) + Q(h)$, donc : $\mathrm{d}Q_p(h) = 2\Phi(h,p)$. Ainsi, vu comme espace vectoriel, l'espace tangent à $\mathscr{N}_0$ en un point p est l'orthogonal de p. (Comme Q est non dégénérée et que p n'est pas nul, c'est un plan : cela traduit que le seul point singulier de $\mathscr{N}_0$ est l'origine.) Vu comme un espace affine, le plan tangent à $\mathscr{N}_0$ en p contient un point x si et seulement si l'on a : $\mathrm{d}Q_p(x-p) = 0$, c'est-à-dire : $\Phi(x,p) = 0$ puisque $\Phi(p,p) = 0$. (Sans surprise, le plan tangent au cône $\mathscr{N}_0$ contient l'origine.) On voit que ces caractérisations sont purement algébriques : on les prend pour définitions pour un corps $\mathbb{K}$ quelconque.

A.3. Définition. Le *plan tangent* au cône quadratique d'équation $Q = 0$ en un point p non nul de ce cône est le plan orthogonal (pour Q) à p. Dans l'espace projectif, la *droite tangente* à la conique d'équation $Q = 0$ dans $\mathbb{P}^2(\mathbb{K})$ est la droite d'équation : $\Phi(p,x) = 0$.

A.4. Points extérieurs et intérieurs, droites sécantes et extérieures

Il saute aux yeux d'un observateur « réel » que l'extérieur d'une ellipse est l'ensemble des points d'où l'on peut mener une tangente à la conique (et même deux). Comme la notion de tangence vient d'être algébrisée, on peut étendre la notion d'extérieur à une conique sur un corps quelconque.

Soit comme ci-dessus une conique non dégénérée $\mathscr{C}$ de $\mathbb{P}^2(\mathbb{K})$. Un point p du plan projectif est de l'un des trois types suivants :

- soit p appartient à $\mathscr{C}$;
- soit p est *extérieur* à $\mathscr{C}$, c'est-à-dire que p appartient à la tangente à $\mathscr{C}$ en un point q distinct de p ; (alors, p n'appartient pas à $\mathscr{C}$: la tangente en q coupe $\mathscr{C}$ en un point double q donc aucun autre point ;)
- soit p est *intérieur* à $\mathscr{C}$, au sens où p n'appartient à aucune tangente à la conique $\mathscr{C}$.

On a une typologie analogue pour les droites de $\mathbb{P}^2(\mathbb{K})$. En effet, une droite D est de l'un des trois types suivants :

- soit D est *tangente* à $\mathscr{C}$ au sens ci-dessus ;
- soit D est *sécante* à $\mathscr{C}$, au sens où D coupe $\mathscr{C}$ en deux points distincts ;
- soit D est *extérieure* à $\mathscr{C}$, c'est-à-dire que D ne coupe pas $\mathscr{C}$.

En effet, l'intersection de D et $\mathscr{C}$ est l'image dans le plan projectif du cône isotrope de la restriction de Q au plan vectoriel P qui définit D : c'est donc un point double, deux points distincts ou le vide, selon que $Q|_P$ est congruente à $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$ ou $\left(\begin{smallmatrix}1&0\\0&-\zeta\end{smallmatrix}\right)$ (où ζ est un élément de $\mathbb{K}^*$ qui n'est pas un carré), qui définissent les trois classes de congruence possibles d'une forme quadratique non nulle sur un plan.

Remarquons que sur un corps algébriquement clos, il n'y a pas de points intérieurs ni de droites extérieures. À l'opposé de ce que l'œil réel suggère, les droites extérieures et les tangentes contiennent en général des points intérieurs sur un corps fini.

A.5. Polarité

Voici une description géométrique de l'orthogonalité, déjà rencontrée dans [H2G2, exercice X-C.15].

Lemme. *Soit p un point de $\mathbb{P}^2(\mathbb{K})$ n'appartenant pas à $\mathscr{C}$ et soit d_1 (resp. d_2) une droite contenant p et sécante à $\mathscr{C}$ en q_1 et q_2 (resp. q_1' et q_2'). Soit r (resp. s) l'intersection des droites (q_1q_1') et (q_2q_2') (resp. (q_1q_2') et (q_2q_1')). Alors la droite (rs) ne dépend que de $\mathscr{C}$ et p mais pas du choix de d_1 et d_2. En effet, c'est la droite projective $p^\perp$ qui correspond au plan orthogonal à p (considéré comme une droite de $\mathbb{K}^3$).*

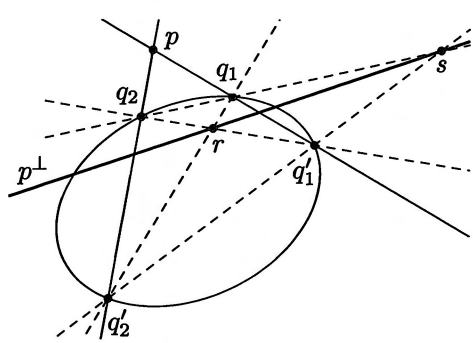
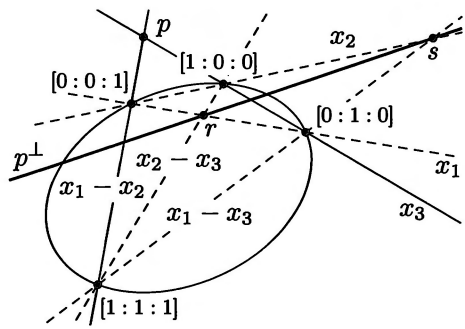


Figure A.1. *Polarité*

Démonstration. Comme les droites sont sécantes et la conique non dégénérée, les points (q_1, q_1', q_2, q_2') forment un repère projectif du plan ([4, définition VI-5.4]). Dans ce repère, ils ont pour coordonnées respectives [1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1] et [1 : 1 : 1]. On complète alors la figure A.1 avec les équations des droites dessinées. On en déduit que p (resp. r, s) a pour coordonnées homogènes [1 : 1 : 0] (resp. [0 : 1 : 1], [1 : 0 : 1]).



De plus, on vérifie sans peine que toute conique contenant q_1, q_1', q_2, q_2' est de la forme $\lambda(x_1 - x_2)x_3 + \mu x_1(x_2 - x_3)$ avec $(\lambda, \mu) \neq (0,0)$ (grouper les quatre points par paires de deux façons différentes et former le produit des équations des droites). La matrice de la forme quadratique correspondante est donnée par :

$$\frac{1}{2}\begin{pmatrix} 0 & \mu & \lambda - \mu \\ \mu & 0 & -\lambda \\ \lambda - \mu & -\lambda & 0 \end{pmatrix},$$

d'où l'on tire que le vecteur $(1,1,0)$ est orthogonal aux vecteurs $(0,1,1)$ et $(1,0,1)$. Cela signifie que les points r et s sont dans l'image de l'orthogonal de p (vu comme droite de $\mathbb{K}^3$). En particulier, pour la conique initiale qui est non dégénérée, l'orthogonal de p est un plan vectoriel ou, dans le plan projectif, la droite projective (rs). □

A.6. Définition. On appelle *polaire* d'un point p par rapport à la conique $\mathscr{C}$ la droite $p^\perp$. Inversement, p est appelé le *pôle* de $p^\perp$.

A.7. Exercice. *Montrer que la polaire d'un point de la conique est une tangente à la conique, que la polaire d'un point extérieur est une sécante et que la polaire d'un point intérieur est une droite extérieure.*

B. Annexe. Classes de conjugaison des groupes linéaires et projectifs sur un corps fini

Soit $\mathbb{F}_q$ un corps fini de cardinal q *impair.*

Nous allons commencer par décrire les classes de conjugaison dans $\mathrm{GL}_2(\mathbb{F}_q)$, ce qui revient à classer les matrices semblables dans $\mathrm{GL}_2(\mathbb{F}_q)$. C'est tout l'objet de la réduction !

B.1. Proposition. *Le groupe* $\mathrm{GL}_2(\mathbb{F}_q)$ *possède* q^2-1 *classes de conjugaison, décrites dans le tableau suivant.*

type	*card. classe*	*nombre classes*	*forme normale*
homothéties	1	$q-1$	$\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix}, \alpha \in \mathbb{F}_q^*$
diagonalisables à v.p. distinctes	$q(q+1)$	$\dfrac{(q-1)(q-2)}{2}$	$\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}, \begin{matrix}\{\alpha,\beta\}\subset\mathbb{F}_q^*,\\ \alpha\neq\beta\end{matrix}$
trigonalisables non diagonalisables	$(q-1)(q+1)$	$(q-1)$	$\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}, \alpha \in \mathbb{F}_q^*$
non trigonalisables	$q(q-1)$	$\dfrac{q(q-1)}{2}$	$\begin{pmatrix}0 & -c\\ 1 & -b\end{pmatrix}, \begin{matrix}b^2-4c\\ \text{non carré}\end{matrix}$

Démonstration. Rappelons que l'ordre de $\mathrm{GL}_2(\mathbb{F}_q)$ est $(q-1)^2q(q+1)$, voir l'exercice I-3.6 ou [H2G2, proposition VIII-1.1].

Chaque homothétie forme une orbite triviale pour la conjugaison, il y en a $(q-1)$ dans $\mathrm{GL}_2(\mathbb{F}_q)$.

Le stabilisateur d'un élément pour l'action par conjugaison est son commutant. Le commutant d'une matrice diagonale à valeur propres distinctes est exactement le sous-groupe des matrices diagonales, qui possède $(q-1)^2$ éléments puisque l'on est dans le groupe des matrices inversibles. La classe de conjugaison a donc pour cardinal

$$\frac{(q-1)^2q(q+1)}{(q-1)^2} = q(q+1).$$

Comme la classe d'une matrice diagonalisable est entièrement déterminée par son spectre, on a $\binom{q-1}{2}$ classes de ce type.

Une matrice trigonalisable et non diagonalisable de $\mathrm{GL}_2(\mathbb{F}_q)$ a un polynôme caractéristique scindé avec une racine double dans $\mathbb{F}_q$. Pour un spectre donné, en dimension 2, il n'y a qu'une seule classe de conjugaison de matrices non diagonalisables. Il y a donc exactement $(q-1)$ classes de ce

type. Le commutant de $A = \left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)$ dans $\mathrm{GL}_2(\mathbb{F}_q)$ est l'ensemble des matrices de la forme $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$ (avec $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$). Le cardinal d'une classe de conjugaison est donc égal à

$$\frac{(q-1)^2 q(q+1)}{(q-1)q} = (q-1)(q+1).$$

Reste le cas d'une matrice A dont le polynôme caractéristique $\chi_A = X^2 + bX + c$ n'est pas scindé. Dans ce cas, χ_A est irréductible sur $\mathbb{F}_q$ et, par le théorème de Cayley-Hamilton, le polynôme caractéristique de A est égal à son polynôme minimal. Ainsi, par [H2G2, proposition III-5.5], A est dans la classe de conjugaison de la matrice compagnon $\left(\begin{smallmatrix} 0 & -c \\ 1 & -b \end{smallmatrix}\right)$. Les classes de conjugaison sont donc complètement caractérisées par le polynôme caractéristique qui est un polynôme de degré 2 non scindé (ce qui revient à dire que le discriminant $b^2 - 4c$ n'est pas un carré de $\mathbb{F}_q$) et unitaire de $\mathbb{F}_q[X]$. On peut les compter par élimination puisqu'il y a q^2 polynômes unitaires de degré 2 et parmi eux $q(q+1)/2$ sont scindés (compter les paires de racines). On trouve donc $q(q-1)/2$ classes de conjugaison. Le cardinal d'une classe de conjugaison peut être calculé de la manière suivante. Comme la matrice A est semblable à une matrice compagnon, la proposition II-2.2 assure que le commutant de A est $\mathbb{F}_q[A]$, qui possède pour base (I_2, A). Comme le polynôme caractéristique de A est irréductible, la matrice A n'a pas de valeurs propres, et donc, les matrices inversibles de la forme $\alpha \mathrm{I}_2 + \beta A$ sont les matrices non nulles de $\mathbb{F}_q[A]$. L'orbite a donc pour cardinal $(q^2-1)(q^2-q)/(q^2-1) = q(q-1)$. □

B.2. Exercice. *Démontrer par une méthode plus directe que le cardinal d'une orbite de matrice non trigonalisable de* $\mathrm{GL}_2(\mathbb{F}_q)$ *est égal à* $q(q-1)$.

On pourra simplement expliciter le commutant d'une matrice compagnon.

B.3. Remarque. Pour des raisons que l'on comprendra (au besoin, on fera semblant), les différents types rencontrés dans le tableau sont appelés respectivement : scalaire, hyperbolique, parabolique et elliptique.

B.4. Tores déployés, tores non déployés

Par [H2G2, proposition II-2.2.1], sur le corps des complexes, l'ensemble des matrices diagonalisables est dense dans l'espace des matrices. En revanche, sur un corps non algébriquement clos, la diagonalisabilité n'est pas chose courante. Nous avons introduit en II-1 la notion de semi-simplicité, qui généralise la notion de diagonalisabilité. Ici, nous allons exprimer la chose autrement, en introduisant la notion de tore déployé, ce qui aura l'avantage de fournir un élément de forme normale pour les orbites de matrices non trigonalisables.

Notations. On note T l'image du morphisme

$$\mathbb{F}_q^* \times \mathbb{F}_q^* \longrightarrow \mathrm{GL}_2(\mathbb{F}_q), \quad (\alpha, \beta) \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

On dit que T est un *tore déployé.*

Ce tore déployé n'est autre que le sous-groupe des matrices diagonales, qui permet d'obtenir une forme normale, à permutation des valeurs propres près. Et par définition toute classe de conjugaison de matrices diagonalisables rencontre le tore déployé en un point si les valeurs propres sont égales, ou deux si elles sont distinctes. Rien de bien nouveau, inutile de s'apesantir.

Notations. On sait qu'il existe, à isomorphisme près, une unique extension du corps $\mathbb{F}_q$ de degré 2, voir [65, §III.2]. Il est noté $\mathbb{F}_{q^2}$ et a pour dimension 2 comme espace vectoriel sur $\mathbb{F}_q$. On choisit une base de $\mathbb{F}_{q^2}$ sur $\mathbb{F}_q$, ce qui donne un isomorphisme d'espaces $\mathbb{F}_{q^2} \simeq \mathbb{F}_q^2$. Pour tout μ de $\mathbb{F}_{q^2}$, on notera T_μ la matrice de multiplication par μ dans cette base. La multiplication par μ est inversible (μ l'est, ne soyons pas bourrins) et l'application de $\mathbb{F}_{q^2}^*$ dans $\mathrm{GL}_2(\mathbb{F}_q)$ qui envoie μ sur T_μ est un morphisme injectif de groupes.

On note $T' = \{T_\mu,\ \mu \in \mathbb{F}_{q^2}\}$. On dit que c'est un *tore non déployé.* Il dépend du choix d'une base $\mathbb{F}_{q^2}$ sur $\mathbb{F}_q$, que nous avons fait une fois pour toutes.

B.5. Proposition. *Le tore non déployé T' est un sous-groupe cyclique d'ordre q^2-1 de $\mathrm{GL}_2(\mathbb{F}_q)$. Tout élément T_μ de T' est soit une homothétie si $\mu \in \mathbb{F}_q$, soit une matrice non trigonalisable de $\mathrm{GL}_2(\mathbb{F}_q)$ si $\mu \notin \mathbb{F}_q$. De plus, toute classe de conjugaison de matrices non trigonalisables rencontre T' deux fois.*

Démonstration. On sait que le groupe multiplicatif d'un corps fini est cyclique, voir [65, théorème III-2.7]. Donc T' est cyclique d'ordre $q^2 - 1$.

Soit μ dans $\mathbb{F}_{q^2}$ tel que le morphisme φ_μ de multiplication par μ possède un vecteur propre. Il existe donc un vecteur propre v dans $\mathbb{F}_{q^2}$ et une valeur propre λ dans $\mathbb{F}_q$ tels que $\mu v = \lambda v$. Donc $\mu = \lambda \in \mathbb{F}_q$ et φ_μ est bien une homothétie.

Reste donc à montrer la dernière assertion. On a vu précédemment qu'une classe de conjugaison de matrices non trigonalisables de $\mathrm{GL}_2(\mathbb{F}_q)$ était caractérisée par son polynôme caractéristique (cette figure dérivative n'est pas tout à fait innocente). De plus, pour tout polynôme P de $\mathbb{F}_q[X]$, $P(\varphi_\mu)$ est nul si et seulement si $P(\mu)$ l'est. Donc, si T_ν (où $\nu \in \mathbb{F}_{q^2}$) est dans la classe de conjugaison fixée par un polynôme caractéristique P, irréductible de degré 2, on a $P(\nu) = 0$. Or, en caractéristique différente de 2,

le polynôme caractéristique P (ce polyptote est, lui, tout à fait fortuit) irréductible de degré 2, possède dans $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ exactement deux racines distinctes, μ et[14] $\bar{\mu}$. Il y a donc au plus deux matrices T_ν dans cette classe de conjugaison. Réciproquement, P est déterminé par μ, puisqu'il s'agit du polynôme annulateur minimal de μ, et donc T_μ est bien dans la classe de conjugaison de polynôme caractéristique P. De même pour $\bar{\mu}$. □

B.6. Remarque. Justifions un peu la terminologie. Au départ, un tore est un espace topologique isomorphe à $\mathbf{S}^1 \times \mathbf{S}^1$. Version groupes : c'est $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. Par extension, c'est n'importe quel groupe de la forme $(\mathbb{R}/\mathbb{Z})^n$ ($n \in \mathbb{N}$). Les séries de Fourier montrent qu'un tel groupe est bien décrit par les polynômes trigonométriques. En effet, avec $n = 1$ pour simplifier, ils forment l'algèbre $\mathbb{C}[\mathbf{t}, \mathbf{t}^{-1}]$, où $\mathbf{t} : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$, $t \mapsto e^{i2\pi t}$; c'est l'algèbre des polynômes de Laurent qui sont exactement les fonctions polynomiales sur $\mathbb{C}^*$.

Dans la théorie des groupes algébriques complexes, un tore est un groupe de la forme $(\mathbb{C}^*)^n$. Un tore réel devrait donc être un groupe de la forme $(\mathbb{R}^*)^n$, décrit par l'algèbre $\mathbb{R}[t, t^{-1}]$.

Bon. Mais s'il s'agit de géométrie algébrique, on devrait identifier $\mathbb{R}/\mathbb{Z}$ au cercle $\mathbf{S}^1$ et les fonctions polynomiales devraient être l'algèbre des polynômes sur le plan quotientée par l'idéal engendré par l'équation du cercle, *i.e.* $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$. Quel lien avec $\mathbb{R}^*$? Si on *étend les scalaires* de $\mathbb{R}$ à $\mathbb{C}$, on trouve le même tore $\mathbb{C}^*$. D'un côté, $\mathbb{C}[t, t^{-1}]$ est bien l'algèbre de $\mathbb{C}^*$. De l'autre, on a des isomorphismes :

$$\mathbb{C}[t, t^{-1}] \simeq \mathbb{C}[x, y]/(x^2 + y^2 - 1), \quad \begin{cases} t \mapsto x + iy, \\ \frac{1}{2}(t + t^{-1}) \leftarrow\!\shortmid\, x, \ \frac{1}{2i}(t - t^{-1}) \leftarrow\!\shortmid\, y. \end{cases}$$

On dit que $\mathbb{R}^*$ et $\mathbb{R}/\mathbb{Z}$ sont deux *formes réelles* de $\mathbb{C}^*$. Un *tore déployé* sur un corps $\mathbb{K}$ est un groupe isomorphe à $(\mathbb{K}^*)^n$ ($n \in \mathbb{N}$). Un *tore non déployé* est un groupe qui n'est pas isomorphe à $(\mathbb{K}^*)^n$ mais qui, lorsque l'on étend les scalaires à une extension $\mathbb{L}$ de $\mathbb{K}$, devient isomorphe à $(\mathbb{L}^*)^n$ ($n \in \mathbb{N}$). On vérifie que le groupe T' ci-dessus est bien un tore non déployé sur $\mathbb{F}_p$.

B.7. Action des homothéties sur les classes de conjugaison

Ce paragraphe est préliminaire au suivant, dans lequel nous étudierons les classes de conjugaison de $\mathrm{PGL}_2(\mathbb{F}_q)$. Commençons tout d'abord par définir l'action du groupe $\mathbb{F}_q^*$ sur l'ensemble des classes de conjugaison de $\mathrm{GL}_2(\mathbb{F}_q)$. Le groupe $\mathbb{F}_q^*$ des homothéties agit sur $\mathrm{GL}_2(\mathbb{F}_q)$ par multiplication, et cette action commute à l'action de $\mathrm{GL}_2(\mathbb{F}_q)$ sur lui-même par conjugaison.

[14] On sait qu'elle peuvent s'écrire μ et μ^q.

Ainsi (rappelons que $[A]$ désigne l'image de la matrice inversible A dans le groupe projectif), on peut définir l'action du groupe des homothéties sur les classes de conjugaison par

$$\lambda \cdot [A] = [\lambda A] \quad \big(\lambda \in \mathbb{F}_q^*,\ A \in \mathrm{GL}_2(\mathbb{F}_q)\big).$$

De plus, on a les relations suivantes entre les polynômes minimaux et entre les polynômes caractéristiques

$$\mu_{\lambda A}(X) = \mu_A(\lambda^{-1}X),\ \chi_{\lambda A}(X) = \chi_A(\lambda^{-1}X).$$

Cela prouve que l'homothétie respecte le type (diagonalisable, non trigonalisable,...) de la classe de conjugaison tel qu'il apparaît dans le tableau de la proposition B.1. On va donc regarder l'action des homothéties type par type. Nous utiliserons pour cela un petit lemme spécifique de la dimension 2.

B.8. Lemme. *Soient A et A' deux éléments de $\mathrm{GL}_2(\mathbb{F}_q)$, ayant pour spectres respectifs* $\mathrm{Spec}(A)$ *et* $\mathrm{Spec}(A')$. *On suppose que A et A' ne sont pas des homothéties. Alors, A et A' sont conjuguées modulo homothéties,* i.e. *il existe $P \in \mathrm{GL}_2(\mathbb{F}_q)$ et $\lambda \in \mathbb{F}_q^*$ tels que $A' = \lambda PAP^{-1}$, si et seulement s'il existe λ dans $\mathbb{F}_q^*$ tel que $\lambda\,\mathrm{Spec}(A) = \mathrm{Spec}(A')$. De plus :*

(i) *si $\mathrm{tr}(A) \neq 0$, le stabilisateur dans $\mathbb{F}_q^*$ de la classe de conjugaison de A est réduit au neutre ;*

(ii) *si $\mathrm{tr}(A) = 0$, le stabilisateur dans $\mathbb{F}_q^*$ de la classe de conjugaison de A est $\{1, -1\}$.*

Démonstration. Au sein de chaque type, toute classe de conjugaison est caractérisée par son spectre : pour les classes de matrices non trigonalisables, c'est montré dans le paragraphe précédent, et pour les autres, c'est clair. La première assertion en découle.

Supposons maintenant λ dans le stabilisateur de la classe de conjugaison de A. On peut donc trouver (dans une extension de $\mathbb{F}_q$) deux valeurs propres de A telles que $\lambda\alpha = \alpha,\ \lambda\beta = \beta$ ou $\lambda\alpha = \beta,\ \lambda\beta = \alpha$. Le premier système donne $\lambda = 1$ puisque $\alpha, \beta \neq 0$. Le second système donne $\lambda = 1$, sauf si $\beta = -\alpha$, auquel cas $\lambda = -1$ est solution. Comme la trace de A est la somme des valeurs propres, nous avons le lemme. □

Comme q est impair, la trace ne peut être nulle que dans deux situations : dans le cas diagonalisable à valeurs propres distinctes et dans le cas non trigonalisable. Dans ces deux cas, nous avons $(q-1)/2$ classes égales modulo homothéties. Hormis ces cas, nous pouvons regrouper $q-1$ classes de conjugaison modulo homothéties. L'invariant total associé à la classe de A de spectre $\mathrm{Spec}(A) = \{\alpha, \beta\}$ est $\{\alpha/\beta, \beta/\alpha\}$.

La classification dans $\mathrm{GL}_2(\mathbb{F}_q)$ pour l'action étudiée est alors immédiate par la proposition B.1.

1. Sur les homothéties : il n'y a plus qu'une classe de conjugaison modulo les homothéties, celle de l'identité ; forme normale : $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$; cardinal $(q-1)$.

2. Sur les matrices diagonalisables à valeurs propres distinctes ; on distingue deux cas :
   (a) la trace est nulle ;
   une seule classe donc, celle de forme normale $\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$;
   cardinal : $q(q+1)(q-1)/2$;
   (b) la trace n'est pas nulle ;
   les classes ont une forme normale $A_\omega = \left(\begin{smallmatrix}\omega&0\\0&1\end{smallmatrix}\right)$, avec $\omega \neq \pm 1$; deux matrices A_ω et $A_{\omega'}$ sont dans la même classe si et seulement si $\omega' = \omega$ ou $\omega' = \omega^{-1}$; il y a donc $(q-3)/2$ telles classes (on retire à $\mathbb{F}_q$ les trois éléments 0, 1 et -1, et l'on en prend un sur deux car $\omega \neq \omega^{-1}$) ; chaque classe contient $q(q+1)(q-1)$ éléments dans $\mathrm{GL}_2(\mathbb{F}_q)$.

3. Sur les matrices trigonalisables non diagonalisables ; une seule classe de forme normale $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$; pour s'en convaincre, on peut noter la formule
$$\begin{pmatrix}\alpha&1\\0&\alpha\end{pmatrix} = \alpha \begin{pmatrix}\alpha^{-1}&0\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}\alpha&0\\0&1\end{pmatrix};$$
   cette classe contient, d'après le tableau qui précède, $(q-1)^2(q+1)$ éléments (dans $\mathrm{GL}_2(\mathbb{F}_q)$).

4. Sur les matrices non trigonalisables ; on distingue deux cas :
   (a) la trace est nulle ;
   une seule classe donc, celle de forme normale $\left(\begin{smallmatrix}0&\zeta\\1&0\end{smallmatrix}\right)$, où ζ est un non carré de $\mathbb{F}_q$ fixé ; cardinal : $q(q-1)^2/2$;
   (b) la trace est non nulle ;
   alors le polynôme caractéristique (irréductible !) est de la forme $X^2 + bX + c'$ avec $b \neq 0$. En multipliant la matrice par un scalaire, on se ramène à une matrice dont le polynôme caractéristique (toujours irréductible) est de la forme $X^2 + X + c$. On a donc $(q-1)/2$ classes dont la forme normale est $\left(\begin{smallmatrix}0&-c\\1&-1\end{smallmatrix}\right)$ avec $1-4c$ non carré, c'est-à-dire $c = \nu\zeta - 1/4$, $\nu \in (\mathbb{F}_q^*)^2$; chaque classe contient $q(q-1)^2$ éléments dans $\mathrm{GL}_2(\mathbb{F}_q)$.

Tout vient donc d'être défriché pour pouvoir traiter le problème plus délicat des classes de conjugaison du groupe projectif $\mathrm{PGL}_2(\mathbb{F}_q)$.

B.9. Proposition. *Le groupe* $\mathrm{PGL}_2(\mathbb{F}_q)$ *admet* $q+2$ *classes de conjugaison, décrites dans le tableau suivant, où* ζ *est un non carré de* $\mathbb{F}_q$ *fixé.*

type	*card. classe*	*nb classes*	*forme normale*	*ordre*
identité	1	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
diagonalisables de trace nulle	$\frac{q(q+1)}{2}$	1	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	2
diagonalisables de trace non nulle	$q(q+1)$	$\frac{q-3}{2}$	$\begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix}, \omega \neq \pm 1$	$d > 2$ $d \mid (q-1)$
trigonalisables non diagonalisables	q^2-1	1	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	p
non trigonalisables de trace nulle	$\frac{q(q-1)}{2}$	1	$\begin{pmatrix} 0 & \zeta \\ 1 & 0 \end{pmatrix}$	2
non trigonalisables de trace non nulle	$q(q-1)$	$\frac{q-1}{2}$	$\begin{pmatrix} 0 & \nu^2\zeta - 1 \\ 1 & -2 \end{pmatrix}, \nu \neq 0$	$d > 2$ $d \mid (q+1)$

Démonstration. Nous avons regroupé les éléments de $\mathrm{GL}_2(\mathbb{F}_q)$ par orbites pour l'action de $\mathbb{F}_q^* \times \mathrm{GL}_2(\mathbb{F}_q)$ donnée par $(\lambda, P) \cdot A = \lambda(PAP^{-1})$. Il suffit donc de voir que, dans $\mathrm{PGL}_2(\mathbb{F}_q)$, la classe $[A']$ de A' est $\mathrm{PGL}_2(\mathbb{F}_q)$-conjuguée à la classe $[A]$ de A si et seulement si A' et A sont dans la même orbite modulo $\mathbb{F}_q^* \times \mathrm{GL}_2(\mathbb{F}_q)$. Cela est clair. De plus, les éléments A tels que $[A]$ est fixé sont dans la même $\mathbb{F}_q^* \times \mathrm{GL}_2(\mathbb{F}_q)$-orbite. Comme il y en a $(q-1)$, on peut donc passer de l'étude précédente à l'étude des classes de conjugaison de $\mathrm{PGL}_2(\mathbb{F}_q)$ en divisant par $(q-1)$ le cardinal de chaque orbite.

Reste à comprendre les ordres des éléments dans la classe de conjugaison. On remarque tout d'abord que l'ordre d'un élément ne dépend que de la classe de conjugaison à laquelle il appartient.

Les ordres sont alors calculés à partir des considérations suivantes.

1. La classe de $\left(\begin{smallmatrix} \omega & 0 \\ 0 & 1 \end{smallmatrix}\right)$ modulo les homothéties est égale à l'ordre de ω dans $\mathbb{F}_q^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. De plus, si ω a même ordre que ω^{-1}.
2. Pour tout α non nul dans $\mathbb{F}_q$, $k \mapsto \left[\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right]$ établit un morphisme injectif du groupe additif $\mathbb{Z}/p\mathbb{Z}$ dans le groupe multiplicatif $\mathrm{PGL}_2(\mathbb{F}_q)$.
3. Le morphisme $\mathbb{F}_{q^2}^* \to \mathrm{GL}_2(\mathbb{F}_q)$ passe au quotient en un morphisme injectif $\mathbb{F}_{q^2}^*/\mathbb{F}_q^* \to \mathrm{PGL}_2(\mathbb{F}_q)$. NB : $\mathbb{F}_{q^2}^*/\mathbb{F}_q^* \simeq (\mathbb{Z}/(q^2-1)\mathbb{Z})/(\mathbb{Z}/(q-1)\mathbb{Z})$ $\simeq \mathbb{Z}/(q+1)\mathbb{Z}$. Cette fois, on regroupe deux par deux les racines conjuguées du polynôme caractéristique et celles-ci ont le même ordre. □

B.10. Remarque. L'isomorphisme exceptionnel $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ illustre que l'étude des classes de conjugaison en caractéristique 2 est spécifique.

Classes de conjugaison de $\mathrm{PSL}_2(\mathbb{F}_q)$

Pour déterminer les classes de conjugaison de $\mathrm{PSL}_2(\mathbb{F}_q)$ à partir de celles de $\mathrm{PGL}_2(\mathbb{F}_q)$, il n'y a qu'un pas, résumé dans le lemme suivant.

B.11. Lemme. *Notons $K_2(\mathbb{F}_q)$ le sous-groupe des matrices de $\mathrm{GL}_2(\mathbb{F}_q)$ dont le déterminant est un carré de $\mathbb{F}_q$. Pour $A \in \mathrm{GL}_2(\mathbb{F}_q)$, on a :*

(i) *l'image $[A]$ de A modulo les homothéties est dans $\mathrm{PSL}_2(\mathbb{F}_q)$ si et seulement si $A \in K_2(\mathbb{F}_q)$,*

(ii) *si $[A] \in \mathrm{PSL}_2(\mathbb{F}_q)$, la classe de conjugaison de $[A]$ dans $\mathrm{PGL}_2(F_q)$ est entièrement incluse dans $\mathrm{PSL}_2(\mathbb{F}_q)$;*

  (a) *elle se scinde en deux classes de conjugaison de $\mathrm{PSL}_2(\mathbb{F}_q)$ si et seulement si le centralisateur de A dans $\mathrm{GL}_2(\mathbb{F}_q)$ est dans $K_2(\mathbb{F}_q)$,*

  (b) *elle reste une seule classe de conjugaison de $\mathrm{PSL}_2(\mathbb{F}_q)$ sinon.*

Démonstration. Par construction, $[A] \in \mathrm{PSL}_2(\mathbb{F}_q)$ si et seulement si $A = \lambda B$, avec $\lambda \in \mathbb{F}_q^*$, $B \in \mathrm{SL}_2(\mathbb{F}_q)$. Donc $\det(A) = \lambda^2$ est bien un carré. Et réciroquement, si $\det(A) = \lambda^2$, alors $\lambda^{-1}A \in \mathrm{SL}_2(\mathbb{F}_q)$.

Maintenant, dans le cas où $[A] \in \mathrm{PSL}_2(\mathbb{F}_q)$, alors, pour tout P de $\mathrm{GL}_2(\mathbb{F}_q)$, $\det(PAP^{-1}) = \det(A)$, qui est un carré. Donc, toute la classe de conjugaison de $[A]$ dans $\mathrm{PGL}_2(F_q)$ est incluse dans $\mathrm{PSL}_2(\mathbb{F}_q)$.

Pour le second point, on rappelle tout d'abord que $\mathrm{SL}_2(\mathbb{F}_q)$ est d'indice 2 dans $\mathrm{GL}_2(\mathbb{F}_q)$. On suppose que le centralisateur de A dans $\mathrm{GL}_2(\mathbb{F}_q)$, et donc le stabilisateur de A pour la conjugaison, est dans le sous-groupe des carrés $K_2(\mathbb{F}_q)$. Alors, d'après le premier point, l'image du stabilisateur S_A de $[A]$ pour l'action de conjugaison de $\mathrm{PGL}_2(\mathbb{F}_q)$ est incluse dans $\mathrm{PSL}_2(\mathbb{F}_q)$. Et comme le sous-groupe $K_2(\mathbb{F}_q)$ est distingué dans $\mathrm{GL}_2(\mathbb{F}_q)$, pour tout B dans la classe de conjugaison de A, le stabilisateur de B, qui est conjugué au stabilisateur de A est aussi dans $K_2(\mathbb{F}_q)$. On sait que $\mathrm{PSL}_2(\mathbb{F}_q) \cdot [B]$ est en bijection avec $\mathrm{PSL}_2(\mathbb{F}_q)/S_B$ qui est de cardinal $\big(\big|\mathrm{PGL}_2(\mathbb{F}_q)\big|/2\big)/|S_B|$. La classe de $[A]$ pour $\mathrm{PGL}_2(\mathbb{F}_q)$ se scinde donc en deux classes de cardinaux égaux.

On suppose que le centralisateur de A dans $\mathrm{GL}_2(\mathbb{F}_q)$ n'est pas dans le sous-groupe des carrés $K_2(\mathbb{F}_q)$. Avec les notations précédentes, l'inclusion de S_A dans $\mathrm{PGL}_2(\mathbb{F}_q)$ fournit un morphisme $S_A \to \mathrm{PGL}_2(\mathbb{F}_q)/\mathrm{PSL}_2(\mathbb{F}_q) \simeq \{1, -1\}$ de noyau $S_A \cap \mathrm{PSL}_2(\mathbb{F}_q)$, d'où une injection $S_A/\big(S_A \cap \mathrm{PSL}_2(\mathbb{F}_q)\big) \to \{1, -1\}$. Comme par hypothèse, son image n'est pas de cardinal 1, il est de cardinal 2. Donc le cardinal de la classe de conjugaison de $[A]$ dans $\mathrm{PSL}_2(\mathbb{F}_q)$ est simplement $\Big|\mathrm{PSL}_2(\mathbb{F}_q)/\big(S_A \cap \mathrm{PSL}_2(\mathbb{F}_q)\big)\Big| = \big|\mathrm{PGL}_2(\mathbb{F}_q)/S_A\big|$, lui-même égal au cardinal de la classe de conjugaison de $[A]$ dans $\mathrm{PGL}_2(\mathbb{F}_q)$. □

B.12. Proposition. *Les classes de conjugaison de* $\mathrm{PSL}_2(\mathbb{F}_q)$ *sont classées dans les tableaux suivants selon que* q *congru à* 1 *ou* 3 *modulo* 4. *(On fixe un élément* $\zeta \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$ *et l'on note* $\heartsuit$ *la condition :* $-\nu^2\zeta + 1 \in (\mathbb{F}_q^*)^2$.*)*

Premier cas : $q \equiv 1 \pmod 4$.

type	*card. classe*	*nb classes*	*forme normale*	*ordre*
identité	1	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
diagonalisables de trace nulle	$\frac{q(q+1)}{2}$	1	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	2
diagonalisables de trace non nulle	$q(q+1)$	$\frac{q-5}{4}$	$\begin{pmatrix} \omega^2 & 0 \\ 0 & 1 \end{pmatrix}, \omega^2 \neq \pm 1$	$d > 2$ $d \mid \frac{q-1}{2}$
trigonalisables non diagonalisables	$\frac{q^2-1}{2}$	2	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	p
non trigonalisables de trace non nulle	$q(q-1)$	$\frac{q-1}{4}$	$\begin{pmatrix} 0 & \nu^2\zeta - 1 \\ 1 & -2 \end{pmatrix}$, $(\heartsuit)$	$d > 1$ $d \mid \frac{q+1}{2}$

Deuxième cas : $q \equiv 3 \pmod 4$.

type	*card. classe*	*nb classes*	*forme normale*	*ordre*
identité	1	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
diagonalisables de trace non nulle	$q(q+1)$	$\frac{q-3}{4}$	$\begin{pmatrix} \omega^2 & 0 \\ 0 & 1 \end{pmatrix}, \omega^2 \neq \pm 1$	$d > 1$ $d \mid \frac{q-1}{2}$
trigonalisables non diagonalisables	$\frac{q^2-1}{2}$	2	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	p
non trigonalisables de trace nulle	$\frac{q(q-1)}{2}$	1	$\begin{pmatrix} 0 & \zeta \\ 1 & 0 \end{pmatrix}$	2
non trigonalisables de trace non nulle	$q(q-1)$	$\frac{q-3}{4}$	$\begin{pmatrix} 0 & \nu^2\zeta - 1 \\ 1 & -2 \end{pmatrix}$, $(\heartsuit)$	$d > 2$ $d \mid \frac{q+1}{2}$

Démonstration. On applique le lemme précédent tout en se référant au tableau des classes de conjugaison de $\mathrm{PGL}_2(\mathbb{F}_q)$. La stratégie est de sélectionner, dans le tableau, les formes normales dont le déterminant est un carré, puis, le cas échéant, voir si le stabilisateur est, ou pas, dans $K_2(\mathbb{F}_q)$.

On a, au cas par cas, les résultats suivants.

1. La matrice $\left(\begin{smallmatrix}\omega & 0\\ 0 & 1\end{smallmatrix}\right)$ est dans $K_2(\mathbb{F}_q)$ si et seulement si ω est un carré non nul. Ces carrés parcourent un groupe cyclique d'ordre $(q-1)/2$. Si $\omega \neq 1$, son stabilisateur est le sous-groupe des matrices diagonales et donc n'est pas inclus dans $K_2(\mathbb{F}_q)$.
2. La matrice $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ est dans $K_2(\mathbb{F}_q)$. Son stabilisateur est le sous-groupe des matrices de la forme $\left(\begin{smallmatrix}a & b\\ 0 & a\end{smallmatrix}\right)$ et donc inclus dans $K_2(\mathbb{F}_q)$.
3. La matrice $\left(\begin{smallmatrix}0 & \nu^2\zeta^{-1}\\ 1 & -2\end{smallmatrix}\right)$ est dans $K_2(\mathbb{F}_q)$ si et seulement si $-\nu^2\zeta+1$ est un carré, avec ν non nul. On est donc ramené à chercher le nombre de solutions de l'équation $\mu^2+\zeta\nu^2=1$. Il s'agit du nombre N_1^ζ avec les notations du §IV-2. Par le lemme IV-2.4, le nombre de solutions est $q-(-\zeta)^{(q-1)/2}$, c'est-à-dire $q+(-1)^{(q-1)/2}$, puisque ζ n'est pas un carré. De plus, ζ n'étant pas un carré, $\mu^2=-\nu^2\zeta+1$ ne s'annule pas et de plus, comme ν est non nul, on obtient finalement $\big(q+(-1)^{(q-1)/2}-2\big)/4$ possibilités.

   Reste à étudier le stabilisateur d'une matrice compagnon non trigonalisable. Une telle matrice A a pour commutant l'espace des $A_{x,y}=xA+yI_2$. De plus, $\det(A_{x,y})$ est la forme quadratique Q en (x,y) telle que $Q(1,-y)$ soit le polynôme caractéristique de $A_{x,y}$, qui est irréductible. La forme Q est donc anisotrope et, en particulier, de rang 2. Or, il est facile de voir, par exemple par le lemme IV-2.4 avec $n=1$, qu'une forme quadratique de rang 2 peut prendre toutes les valeurs possibles de $\mathbb{F}_q$. On a donc montré que le stabilisateur d'une matrice non trigonalisable ne peut être inclus dans $K_2(\mathbb{F}_q)$.

Après cette étude, il reste à distinguer selon que -1 est un carré ou pas.

Dans le cas où q est congru à 1 modulo 4, on sait que -1 est un carré. On a donc toute la classe des matrices diagonalisables de trace nulle. En revanche, la classe des non trigonalisables de trace nulle n'est pas dans $\mathrm{PSL}_2(\mathbb{F}_q)$. On compte

$$\frac{1}{4}\big(q+(-1)^{(q-1)/2}-2\big)=\frac{q-1}{4}$$

formes normales et donc $(q-1)/4$ classes de conjugaison de non trigonalisables.

Dans le cas où q est congru à 3 modulo 4, on sait que -1 n'est pas un carré. On a donc toute la classe des matrices non trigonalisables de trace nulle. En revanche la classe des diagonalisables de trace nulle n'est pas dans $\mathrm{PSL}_2(\mathbb{F}_q)$.

Le calcul des nombres de classes et des cardinaux de classes se fait alors automatiquement avec le lemme.

Pour ce qui est des ordres, la seule difficulté se situe au niveau des matrices diagonalisables (resp. non trigonalisables). Il suffit de constater que ces

matrices, dont on a vu précédemment qu'elles appartiennent à un groupe cyclique d'ordre $q-1$ (resp. $q+1$), se situent maintenant, en vertu de la condition, $\det(A) \in (\mathbb{F}_q^*)^2$ dans un sous-groupe d'indice 2 et donc dans un sous-groupe cyclique d'ordre $(q-1)/2$ (resp. $(q+1)/2$). □

B.13. Exercice. *Montrer que* $\mathrm{SL}_2(\mathbb{F}_q)$ *possède* $q+4$ *classes de conjugaison.*

Avec la terminologie de la remarque B.3, on a : deux classes d'homothéties, à savoir I_2 et $-\mathrm{I}_2$; quatre classes de paraboliques ; si q est congru à 1 (resp. à 3) modulo 4, $(q-3)/2$ classes d'elliptiques (resp. hyperboliques) et $(q-1)/2$ classes de d'hyperboliques (resp. elliptiques).

C. Petits arbres ternaires

Une fois n'est pas coutume, voici, dans la figure C.1, la solution graphique de l'exercice 5.29.

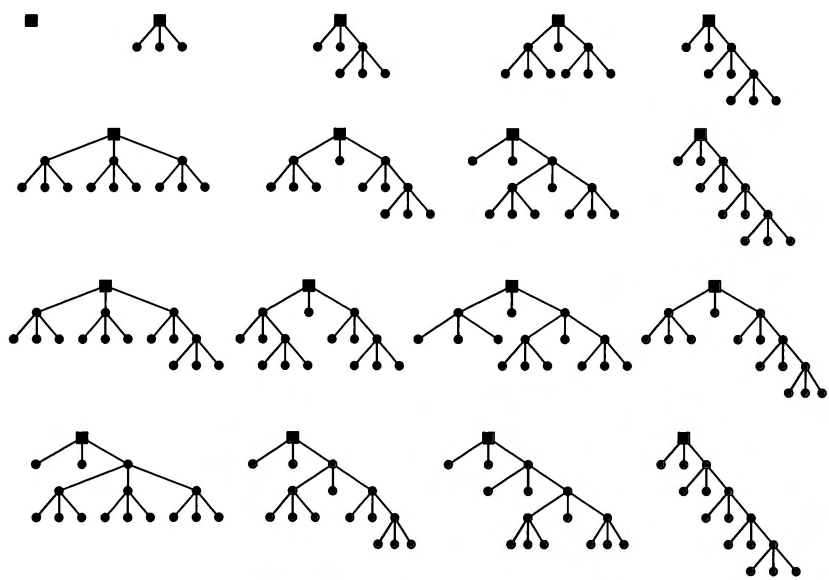


Figure C.1. *Arbres ternaires ayant au plus cinq sommets internes*

D. Exercices du chapitre V

D.1. Exercice (Graphes de Paley)

Soit q une puissance d'un nombre premier qui est congrue à 1 modulo 4. On considère le graphe suivant, appelé graphe de Paley. *Les sommets du graphe sont les éléments de $\mathbb{F}_q$. Deux sommets x et y sont reliés si $x-y$ est un carré non nul de $\mathbb{F}_q$.*

1. *Montrer que chaque sommet est relié à $(q-1)/2$ sommets.*

   C'est le nombre de carrés non nuls.

2. *On considère deux sommets distincts. Montrer que ces sommets sont reliés à $(q-1)/4$ sommets communs.*

   Par le corollaire IV-2.6, il y a $q-1$ éléments dans la nappe quadratique $x^2-y^2=k$, quelque soit k non nul.

Configurations

D.2. Exercice (Configurations et géométrie projective)

On fixe un entier m et deux entiers r et s tels que $r<s\leqslant m$. On considère la configuration suivante : l'ensemble des points est la grassmannienne des sous-espaces projectifs de dimension r de $\mathbb{P}^m(\mathbb{F}_q)$, l'ensemble des lignes est la grassmannienne des sous-espaces projectifs de dimension s de $\mathbb{P}^m(\mathbb{F}_q)$. Un point F est sur une ligne F' si $F\subset F'$ (en tant que sous-espaces).

1. *Montrer que l'on a bien une configuration de type (n_α,ℓ_γ), avec*

$$n=\begin{bmatrix}m+1\\r+1\end{bmatrix}_q,\ \alpha=\begin{bmatrix}m-r\\s-r\end{bmatrix}_q,\ \ell=\begin{bmatrix}m+1\\s+1\end{bmatrix}_q,\ \gamma=\begin{bmatrix}s+1\\r+1\end{bmatrix}_q.$$

2. *On note $\mathscr{C}(m,r,s;q)$ la configuration précédente. Montrer que le dual de $\mathscr{C}(m,r,s;q)$ est $\mathscr{C}(m,m-s-1,m-r-1;q)$.*

3. *Dessiner la configuration « minimale » $\mathscr{C}(2,0,1;2)$ et découvrir ou reconnaître le* plan de Fano.

4. *Utiliser la proposition IV-3.5 pour construire des configurations analogues avec des grassmanniennes isotropes.*

D.3. Exercice. *Soit p un nombre premier impair. On considère la configuration suivante : l'ensemble des points est l'ensemble des classes à gauche de sous-groupes d'ordre p de $(\mathbb{Z}/p\mathbb{Z})^2$, l'ensemble des lignes est l'ensemble $(\mathbb{Z}/p\mathbb{Z})^2$ lui-même. Un point H est sur une ligne h si $h\in H$. Montrer que l'on définit bien une configuration et qu'elle est de type $\big(p(p+1)_p,(p^2)_{p+1}\big)$.*

D.4. Exercice (Groupe de la configuration de Fano)

Le but de l'exercice est de montrer que le groupe de la configuration de Fano, voir figure 5.3, est le groupe $\mathrm{GL}_3(\mathbb{F}_2)$*, sans utiliser le théorème fondamental de la géométrie projective.*

1. *Montrer que l'on peut réaliser le plan de Fano de la manière suivante : les points de la configuration sont les vecteurs de* $\mathbb{F}_2^3 \setminus \{0\}$*, les lignes sont les droites vectorielles de* $\mathbb{F}_2^3$ *et un point appartient à une ligne si le vecteur correspondant au point est sur la droite vectorielle associée à la ligne.*
2. *Montrer que si un point* p *est aligné avec le point* p'*, alors le troisième point de la ligne contenant* p *et* p' *est* $p + p'$*.*
3. *En déduire que le groupe d'automorphismes de la configuration de Fano est le sous-groupe de* $\mathfrak{S}(\mathbb{F}_2^3 \setminus \{0\})$ *constitué des permutations qui respectent l'addition de deux vecteurs distincts de* $\mathbb{F}_2^3 \setminus \{0\}$*.*
4. *Conclure.*

D.5. Exercice (Triangles autopolaires spéciaux sur $\mathbb{F}_7$)

Dans cet exercice, on appelle triangle un triangle autopolaire spécial de $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_7)$ *au sens de la définition 2.13 avec* $q = 7$*.*

1. *Vérifier qu'il existe dans* $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_7)$ *exactement quatorze triangles.*

   Voir la proposition 2.16.
2. *Montrer que le groupe* $\mathrm{PGL}_2(\mathbb{F}_7)$ *(resp.* $\mathrm{PSL}_2(\mathbb{F}_7)$*) agit sur les triangles avec une orbite (resp. deux orbites).*

   À défaut de trouver un argument conceptuel, on pourra toujours énumérer les triangles.
3. *On dit que deux triangles sont* adjacents *s'ils ont un sommet commun. Montrer qu'un triangle est adjacent à exactement trois triangles.*

   La polaire d'un sommet contient $(7 - 1)/2$ points qui se groupent en deux paires.
4. *On construit une configuration dont les points forment une orbite de triangles sous* $\mathrm{PSL}_2(\mathbb{F}_7)$*, les lignes forment l'autre orbite et l'incidence est l'adjacence. Montrer que la configuration obtenue est le plan de Fano (exercice D.4).*
5. *En déduire un isomorphisme* $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{PGL}_3(\mathbb{F}_2)$*.*

Voir aussi le §VII-4, le théorème VII-4.1 et, pour réconcilier les deux points de vue, l'exercice VII-B.6.

Autres configurations

D.6. Exercice (Configuration de Möbius-Kantor)

On considère la configuration de Möbius-Kantor *de type* $(8_3, 8_3)$ *décrite dans la figure de gauche.*

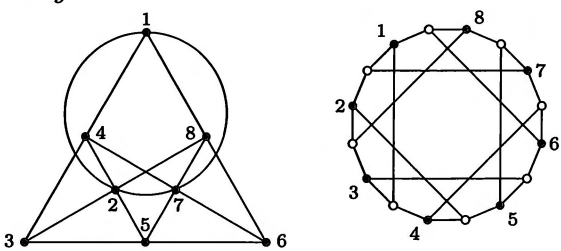


Figure D.1. *Configuration de Möbius-Kantor et son graphe d'incidence*

1. *Vérifier que la figure de droite est bien le graphe d'incidence de la configuration de Möbius-Kantor : les sommets blancs correspondent aux lignes et il y a une arête entre un point et une ligne s'ils sont incidents.*
2. *Exhiber un élément d'ordre* 8 *dans le groupe de symétries G. En particulier, le groupe de symétrie est transitif sur les sommets.*
3. *Montrer que le stabilisateur G_1 du sommet* 1 *est isomorphe à $\mathfrak{S}_3$.*
   Une symétrie qui fixe 1 fixe aussi 5 (pourquoi ?). L'action sur les droites contenant 1 induit un morphisme de G_1 vers $\mathfrak{S}_3$. Montrer qu'il est surjectif : l'axe de symétrie de la figure montre que (48)(36)(27) induit un automorphisme g_1 de la configuration, il suffit d'en exhiber un autre qui permute les lignes (134) et (127). Montrer qu'il est injectif : un élément de G_1 qui stabilise la droite (127) permute les points 2 et 7 ou les fixe : montrer que s'il les fixe, c'est l'identité et conclure grâce à g_1.
4. *En déduire que cette configuration admet quarante-huit symétries.*
5. *Constater que pour tout point p de la configuration, il existe un unique point p^* qui n'est pas sur une ligne contenant p.*
6. *Vérifier que la permutation* (15)(26)(37)(48) *des sommets induit une symétrie z de G. En constatant que z permute les paires $\{p, p^*\}$, montrer que z est central. Le vérifier par un calcul direct à l'aide des générateurs de G.*
7. *Montrer que l'action de G sur les sommets induit une action transitive sur l'ensemble des paires de points $\{p, p^*\}$ ($p \in \{1, \ldots, 8\}$). Montrer que cette action induit un isomorphisme : $G/\langle z\rangle \simeq \mathfrak{S}_4$.*
8. *On rencontrera au §XI-6 le groupe $\tilde{\mathfrak{S}}_4$, qui possède une involution centrale z et dont le quotient par $\langle z\rangle$ est $\mathfrak{S}_4$. Montrer cependant que G n'est pas isomorphe au groupe $\tilde{\mathfrak{S}}_4$.*
   D'un côté, on a mis en évidence plusieurs involutions dans G. D'autre part, $\tilde{\mathfrak{S}}_4$ n'a, en tant que sous-groupe de $\mathrm{SL}_2(\mathbb{C})$, qu'un seul élément d'ordre 2. La structure complète de G sera élucidée dans l'exercice D.7.

9. *Montrer qu'il n'existe, à isomorphisme près, qu'une seule configuration de type* $(8_3, 8_3)$.
   Chaque point $p \in \{1, \dots, 8\}$ est relié à tous les autres sauf un que l'on note p^*. On choisit un point 1 et l'on nomme arbitrairement les points des lignes qui le contiennent : (127), (134) et (168), de sorte que $1^* = 5$. Le point 2 est relié à 7 et à trois des quatre autres, c'est-à-dire tous sauf 2^* que l'on nomme 6. On a donc deux droites (238) et (245) (quitte à permuter 3 et 4). Le point 3 est relié à 1, 2, 4 et 8 ; comme $5^* = 1$ et $6^* = 2$, on voit que $3^* = 7$, d'où une droite (356). Enfin, on vérifie que $4^* = 8$, d'où une droite (467) et une dernière droite (578).
10. *Vérifier que les points suivants de* $\mathbb{P}^2(\mathbb{C})$ *sont reliés par huit droites et forment la configuration précédente :* $[1,0,0]$, $[0,0,1]$, $[\omega,-1,1]$, $[-1,0,1]$, $[-1,\omega^2,1]$, $[1,\omega,0]$, $[0,1,0]$, $[0,-1,1]$ *où* $\omega = e^{2i\pi/3}$.

Cet exercice est inspiré de [68, §5.3.2]. On y apprend que cette configuration n'a pas de réalisation par des points et des droites du plan réel. La source est probablement [18, §5].

D.7. Exercice (Une configuration affine)

Soit q le cardinal d'un corps fini $\mathbb{F}_q$. On considère la configuration $\mathscr{C}_q$ définie ainsi : l'ensemble des points est $\mathbb{F}_q^2 \setminus \{0\}$; les lignes sont les droites affines de $\mathbb{F}_q^2$ qui ne contiennent pas l'origine 0. On note par ailleurs $\widehat{\mathscr{C}_q}$ la configuration dont les points sont ceux de $\mathbb{F}_q^2$ et les lignes sont toutes les droites affines.

1. *Vérifier que $\mathscr{C}_q$ est une configuration de type $\big((q^2-1)_q, (q^2-1)_q\big)$ et injecter $\mathrm{GL}_2(\mathbb{F}_q)$ dans son groupe de symétrie.*
   Une application linéaire préserve les droites affines et fixe l'origine : si une droite ne contient pas l'origine, son image ne la contient pas non plus.
2. *Montrer que tout automorphisme g de $\mathscr{C}_q$ se prolonge de façon unique en un automorphisme $\hat{g}$ de $\widehat{\mathscr{C}_q}$ qui fixe 0.*
   Pour tout point x de $\mathbb{F}_q^2 \setminus \{0\}$, il y a exactement $q-1$ points non alignés avec x au sens de $\mathscr{C}_q$, les kx $(k \in \mathbb{F}_q^*)$. La droite affine $\mathbb{F}_q x$ est donc préservée par g.
3. *À l'aide du « théorème fondamental de la géométrie affine » ([4, exercice I-67]), montrer que $\hat{g}$ est une application affine de $\mathbb{F}_q^2$.*
4. *En déduire que G est naturellement isomorphe à $\mathrm{GL}_2(\mathbb{F}_q)$.*
   Dans le groupe affine, le fixateur d'un point est isomorphe au groupe linéaire.

En prenant $q = 3$, on voit que le groupe de symétries de la configuration de Möbius-Kantor est $\mathrm{GL}_2(\mathbb{F}_3)$. Voir le §5 de [18].

D.8. Exercice (Graphes fortement réguliers)

Montrer que la configuration $\mathscr{C}_5'$ de Desargues (donc !) possède la propriété de régularité suivante :

Il existe deux constantes k_1 et k_2 telles que pour toute paire de points distincts $\{P, P'\}$, on ait exactement k_1 (resp. k_2) points alignés avec P et P' lorsque ceux-ci sont (resp. ne sont pas) alignés.

Par la proposition 2.2, la droite engendrée par deux points (distincts) P et P' de $\mathscr{D}^*$ dans $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_5)$ correspond à un plan, disons, F, de type $\mathscr{P}$ ou $\mathscr{E}$ dans $\mathfrak{sl}_2(\mathbb{F}_5)$ (il ne peut pas être de type $\mathscr{T}$). S'ils sont non alignés dans la configuration $\mathscr{C}_5'$, alors, par élimination, ce plan est de type $\mathscr{P}$. De plus, on voit facilement par la proposition 2.9, que $|F \cap \mathscr{D}^*| = 2$. Donc, si l'on se fixe une autre paire de points non alignés $\{P_0, P_0'\}$ dans un plan F_0, il existe une isométrie de F_0 vers F qui envoie $\{P_0, P_0'\}$ vers $\{P, P'\}$. Donc, le théorème de Witt assure qu'il existe σ dans $\mathrm{O}(Q)$ qui envoie une paire de points non alignés $\{P_0, P_0'\}$ vers $\{P, P'\}$. Alors, σ réalise une bijection entre les points communs alignés de $\{P_0, P_0'\}$ et les points communs alignés de $\{P, P'\}$. Si P et P' sont alignés, le résultat s'obtient de façon assez analogue : il y a trois paires par plan, et $\mathrm{O}(Q \mid F)$ agit, par cardinalité, de façon transitive sur les paires.

Configuration de Cremona-Richmond et applications

D.9. Exercice (Configuration de Cremona-Richmond et ses automorphismes)

On considère la configuration suivante : les points sont les paires d'éléments de $E = \{a, b, c, d, e, f\}$; les lignes sont les partitions de E en trois paires. Un point p est incident à une ligne P si $p \in P$.

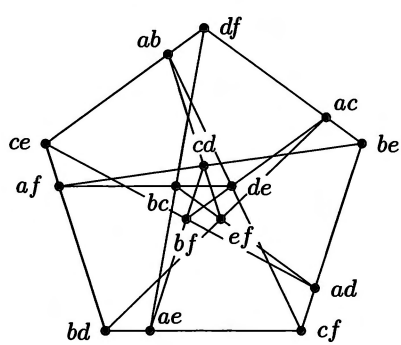


Figure D.2. *Configuration de Cremona-Richmond*

1. *Montrer que l'on obtient bien une configuration de type* $(15_3, 15_3)$.
   Tout repose sur le miracle numérique : $\binom{6}{2} = \binom{6}{2}\binom{4}{2}\binom{2}{2}/3!$.

2. *Montrer que la configuration est autoduale.*
   Pour construire la bijection de la configuration de Cremona-Richmond vers sa duale sans mal, on pourra commencer par définir la transformation en envoyant les points de l'étoile intérieure en lignes du pentagone extérieur. Le reste de la configuration duale s'en déduit par une mécanique lente, mais sûre : chaque fois que deux points alignés sont envoyés sur deux lignes concourantes, le troisième point de l'alignement est envoyé sur la troisième ligne concourante.
3. *Montrer que le groupe $\mathfrak{S}_6$ agit naturellement sur cette configuration et que l'action ainsi définie est fidèle.*
   L'action de $\mathfrak{S}_6$ sur E induit une action sur la configuration. Comme tout élément de E se réalise comme intersection de deux paires, l'action est fidèle.
4. *Montrer que le groupe d'automorphismes de cette configuration est $\mathfrak{S}_6$.*
   Il suffit de montrer que le groupe d'automorphismes est d'ordre inférieur à 6!. On se donne un point p, il peut être envoyé sur au plus quinze points. Sur une première ligne partant de p, on choisit un point q, il peut être envoyé sur au plus six points. Sur une deuxième ligne partant de p, un point r peut alors être envoyé sur au plus quatre points. On fixe donc p, q et r. Soient q' et r' les deux points colinéaires à la fois à q et r, autres que p. Alors q' et r' sont simultanément alignés à q et r et un point s aligné à p. On montre ainsi que le fixateur de (p,q,r) fixe s et donc les trois lignes partant de p. De plus, il envoie q' en q' ou r'. Ensuite, on montre à l'aide du graphique que le fixateur de (p,q,r,q') est trivial. Le groupe d'automorphismes possède donc au plus $15\times 6\times 4\times 2 = 6!$ automorphismes.
5. *(Aparté graphique.) Montrer que sur la figure, le rapport entre les longueurs des côtés des deux pentagones (non étoilés) est*
$$\frac{1}{2}\sqrt{50\sqrt{5}+115}-\frac{3}{2}\sqrt{5}-4.$$

D.10. Exercice (Application à l'isomorphisme exceptionnel $\mathfrak{S}_6 \simeq \mathrm{Sp}_4(\mathbb{F}_2)$). *On va utiliser ici la configuration de Cremona-Richmond pour exhiber un isomorphisme exceptionnel entre $\mathfrak{S}_6$ et $\mathrm{Sp}_4(\mathbb{F}_2)$.*

1. *Montrer en utilisant l'exercice IV-A.10 que $\mathrm{Sp}_4(\mathbb{F}_2)$ agit fidèlement sur la configuration de Cremona-Richmond.*
   Par l'exercice IV-A.10, on réalise la configuration de Cremona-Richmond de la manière suivante : les points sont des vecteurs non nuls de l'espace $\overline{V}_0 \simeq \mathbb{F}_2^4$, les lignes sont les plans totalement isotropes pour la forme symplectique ω et un point appartient à une ligne si le vecteur correspondant appartient au plan. Le groupe $\mathrm{Sp}_4(\mathbb{F}_2)$ agit donc sur la

configuration. L'action de $\mathrm{Sp}_4(\mathbb{F}_2)$ est fidèle puisque si un morphisme fixe tous les vecteurs non nuls, il s'agit de l'identité.

2. *En déduire l'isomorphisme exceptionnel* $\mathrm{Sp}_4(\mathbb{F}_2) \simeq \mathfrak{S}_6$.

   On a une injection par ce qui précède. Et l'égalité des cardinaux provient de l'exercice IV-A.8.

D.11. Exercice (Application aux automorphismes extérieurs de $\mathfrak{S}_6$). *On rappelle que la configuration de Cremona-Richmond est autoduale. On va utiliser cette dualité pour construire un automorphisme intérieur de* $\mathfrak{S}_6$ *(quoique l'on eût pu faire le contraire...)*

1. *Montrer que l'on peut réaliser la configuration de Cremona-Richmond de la manière qui suit : les points de la configuration sont les transpositions de* $\mathfrak{S}_6$*, les lignes en sont les triples transpositions,* i.e. *les produits de trois transpositions deux à deux disjointes. Un point est sur une ligne si le point (donc la transposition) est un cycle de la décomposition en cycles de la triple transposition correspondant à la ligne.*

   C'est la traduction immédiate de la configuration.

2. *Montrer que chaque transposition de* $\mathfrak{S}_6$ *agit par conjugaison comme automorphisme de la configuration ainsi réalisée. Montrer également que toute triple transposition agit par conjugaison comme un automorphisme de la configuration duale (dont les points sont les triples transpositions).*

3. *En déduire que la dualité de la configuration induit un automorphisme extérieur de* $\mathfrak{S}_6$.

   Un isomorphisme entre la configuration et sa duale peut être vu comme une application entre l'ensemble des transpositions et l'ensemble des triples transpositions. La conjugaison par une transposition est transformée, par transport de structure, en la conjugaison par son image. Par la proposition I-B.7, cela se prolonge en un automorphisme de $\mathfrak{S}_6$, nécessairement extérieur puisque l'image d'une transposition n'en est pas une.

Il est conseillé de lire le livre [68].

D.12. Exercice (Autre construction d'un automorphisme extérieur de $\mathfrak{S}_6$)

On se propose de construire un automorphisme extérieur de $\mathfrak{S}_6$ *selon la méthode classique tirée de [65].*

1. *Montrer que l'action de* $\mathrm{GL}_2(\mathbb{F}_5)$ *sur les six droites de* $\mathbb{P}^1(\mathbb{F}_5)$ *est transitive et fournit un morphisme de* $\mathrm{GL}_2(\mathbb{F}_5)$ *dans* $\mathfrak{S}_6$.

2. *Soit $H \subset \mathfrak{S}_6$ l'image de ce morphisme. Montrer que H est d'indice* 6 *dans $\mathfrak{S}_6$ et donc, que l'action à gauche de $\mathfrak{S}_6$ sur $\mathfrak{S}_6/H$ fournit un morphisme injectif ψ de $\mathfrak{S}_6$ sur lui-même.*

   Le sous-groupe H est d'ordre $|\mathrm{PGL}_2(\mathbb{F}_5)| = (5^2-1)(5^2-5)/(5-1) = 120$. Il est donc bien d'indice 6. L'action à gauche sur les classes fournit donc un morphisme de $\mathfrak{S}_6$ dans $\mathfrak{S}_6$. Son noyau est un sous-groupe distingué de $\mathfrak{S}_6$, soit donc $\{e\}$, $\mathfrak{A}_6$, ou $\mathfrak{S}_6$. De plus, son noyau envoie la classe H de e sur elle-même, donc son noyau est contenu dans H. Il est donc trivial.

3. *Montrer que le sous-groupe $\psi(H)$ de $\mathfrak{S}_6$ n'agit pas transitivement pour l'action naturelle de $\mathfrak{S}_6$. En déduire que ψ n'est pas un automorphisme intérieur.*

   Le sous-groupe $\psi(H)$ fixe H, d'où la première assertion. Comme H est transitif (d'après la première question), si ψ était intérieur, $\psi(H)$ le serait aussi.

Les femmes sont beaucoup plus pragmatiques que nous,
elles savent que l'amour n'existe pas et que seules les preuves existent.
Christian Vincent, *La discrète*, 1990.

Chapitre VI

Encores sur les groupes de Lie classiques et isomorphismes exceptionnels

On retrouve ici une des thématiques au cœur du tome premier : les groupes de Lie. Les groupes de Lie sont des groupes munis d'une structure différentielle compatible, dont on ne peut que récolter les bienfaits : la linéarisation, c'est-à-dire ramener un problème de groupes à un problème linéaire [H2G2, annexe IX-B] d'*algèbres de Lie* (voir [H2G2, annexe IX-B]), ou bien l'utilisation du théorème d'inversion locale, dont la puissance se trouve démultipliée dans le contexte des morphismes de groupes. De plus, il n'y a rien de plus simple que de montrer que les groupes utilisés sont « de Lie », du moins si l'on s'autorise à utiliser le théorème de Cartan ([60, §3.4]), selon lequel tout sous-groupe fermé de $\mathrm{GL}_n(\mathbb{K})$ ($\mathbb{K} = \mathbb{C}$ ou $\mathbb{R}$) est un groupe de Lie.

Dans le tome premier, nous avions rencontré le groupe linéaire, le groupe spécial linéaire et les groupes orthogonaux. Pour achever l'étude des groupes de Lie dits « classiques », il nous restait encore à voir le groupe symplectique. Ses propriétés topologiques, sa décomposition polaire, son centre et son algèbre de Lie sont présentés ci-après, dans une première partie.

La théorie de Lie se prête bien à la mise en évidence d'isomorphismes exceptionnels, puisque, comme on l'a déjà vu dans [H2G2, chapitre IX], la surjectivité des morphismes se montre en un claquement de doigts. On présente donc trois isomorphismes « exceptionnels », et, puisque tout ce qui

est en haut est comme ce qui est en bas[1], nous donnons une interprétation de ces isomorphismes en termes géométriques, plus précisément, en termes de plongement classique de variétés projectives.

Nous continuons à exploiter les isomorphismes exceptionnels dans le cas de l'isomorphisme $\mathrm{SO}_0(3,1) \simeq \mathrm{PSL}_2(\mathbb{C})$, qui permet de visiter les cercles du plan avec un nouveau regard, comme cela a déjà été fait dans [H2G2, chapitre XI]. Cette fois-ci, on classifie les faisceaux de cercles modulo $\mathrm{PSL}_2(\mathbb{C})$, via l'action de $\mathrm{SO}_0(3,1)$ sur la grassmannienne des plans de $\mathbb{R}^4$. Le théorème de Witt montre que cette classification a pour invariant la « signature » du plan ; il n'est d'ailleurs pas beaucoup plus difficile de prouver le théorème dans la généralité de l'action de $\mathrm{SO}_0(s,t)$ sur la grassmannienne. On retrouve alors la classification classique des faisceaux, ce qui permet de voir enfin orbites, formes normales et dégénérescences avec de jolis dessins.

1. Études du groupe symplectique

Nous réunissons ici quelques éléments d'étude du groupe symplectique, déjà obtenus en exercices dans les chapitres V, VII et IX du tome premier.

Rappelons qu'une *forme symplectique* sur un espace vectoriel de dimension finie est une forme bilinéaire alternée et non dégénérée. Par [H2G2, proposition V-4.1], nous savons que de telles formes ne peuvent exister que sur un espace de dimension paire, et que dans ce cas, elles constituent une seule orbite pour la congruence.

Le *groupe symplectique* d'un espace vectoriel de dimension paire est défini comme le groupe des automorphismes qui stabilisent une forme symplectique. D'après la remarque précédente, il ne dépend à isomorphisme près que de la dimension de l'espace (et de la nature du corps !).

Nous nous intéresserons principalement au groupe symplectique complexe, qui possède une structure de groupe de Lie, et dont nous étudierons les propriétés topologiques à l'aide d'une décomposition polaire adaptée. Nous indiquerons ensuite les propriétés plus générales du groupe symplectique sur les autres corps.

1.1. Groupe symplectique complexe et bases symplectiques

On travaille sur $\mathbb{C}$ afin de passer rapidement à des problèmes de nature topologique, mais les résultats préliminaires de ce paragraphe sont valables sur tout corps. On fixe un entier naturel non nul n et l'on considère l'espace $\mathbb{C}^{2n}$ muni de sa base canonique. On identifiera donc sans tabou les automorphismes de $\mathbb{C}^{2n}$ aux matrices de $\mathscr{M}_{2n}(\mathbb{C})$.

[1] Pour citer la *Table d'émeraude*, mais aussi John Difool.

Nous espérons ne froisser personne en adoptant les notations suivantes : on note J (ou, s'il est nécessaire de rappeler la dimension, J_n) la matrice de $\mathscr{M}_{2n}(\mathbb{C})$

$$J = \begin{pmatrix} 0_n & -\mathrm{I}_n \\ \mathrm{I}_n & 0_n \end{pmatrix}.$$

Soit ω la forme alternée sur $\mathbb{C}^{2n}$ dont la matrice dans la base canonique de $\mathbb{C}^{2n}$ est J. Elle sera appelée *structure symplectique canonique* de $\mathbb{C}^{2n}$.

On appelle *groupe symplectique* le groupe des automorphismes qui laissent la forme ω invariante. En identifiant les automorphismes de $\mathbb{C}^{2n}$ aux matrices inversibles de $\mathscr{M}_{2n}(\mathbb{C})$, via la base canonique, on l'identifie au groupe

$$\mathrm{Sp}_{2n}(\mathbb{C}) = \left\{P \in \mathrm{GL}_{2n}(\mathbb{K}),\ {}^tPJP = J\right\}.$$

Notons que l'on a : $J^{-1} = {}^tJ = J^\star = -J$. Cette propriété particulière, qui contribue au fait que la matrice J a été choisie comme représentante de forme normale de son orbite de congruence, implique en particulier que le groupe $\mathrm{Sp}_{2n}(\mathbb{C})$ est stable par transposition et par passage à l'adjoint $\star$: $P \mapsto P^\star$.

En effet, si ${}^tPJP = J$, alors, en prenant l'inverse, on obtient $P^{-1}J\,{}^tP^{-1} = J$ et donc ${}^tP^{-1} \in \mathrm{Sp}_{2n}(\mathbb{C})$, ce qui implique ${}^tP \in \mathrm{Sp}_{2n}(\mathbb{C})$. L'assertion sur l'adjoint en résulte car la conjugaison est un morphisme d'algèbres.

Notons aussi que, pour le moment, le déterminant d'un élément P de $\mathrm{Sp}_{2n}(\mathbb{C})$ vaut clairement ± 1 : prendre le déterminant dans la relation qui définit $\mathrm{Sp}_{2n}(\mathbb{C})$ ramène à résoudre $\det(P)^2 = 1$. Nous verrons plus tard qu'en réalité, $\mathrm{Sp}_{2n}(\mathbb{C})$ est un sous-groupe du groupe unimodulaire[2] $\mathrm{SL}_{2n}(\mathbb{C})$: voir le corollaire 1.21.

Il est déjà temps d'introduire le « repère » adapté au groupe symplectique, voir le tableau de [H2G2, annexe II-E] : la base symplectique.

Une base $\mathbf{e} = (e_1, e_2, \ldots, e_n, e_{n+1}, e_{n+2}, \ldots, e_{2n})$ vérifiant

$$\forall i \in \{1, \ldots, n\},\ \forall j \in \{1, \ldots, 2n\},\quad \omega(e_i, e_j) = -\delta_{i+n,j},$$

est appellée *base symplectique*.

La base canonique de $\mathbb{C}^{2n}$ est une base symplectique, ce qui assure déjà l'existence de telles bases. Voici dans la proposition suivante un petit florilège de résultats, bien attendus, qui relient le groupe symplectique et l'ensemble des bases symplectiques.

1.2. Proposition

(i) *Soit* $\mathbf{e}$ *une base symplectique de* $\mathbb{C}^{2n}$. *Un endomorphisme* P *de* $\mathbb{C}^{2n}$ *est dans* $\mathrm{Sp}_{2n}(\mathbb{C})$ *si et seulement si* P *envoie* $\mathbf{e}$ *sur une base symplectique.*

[2] Il n'y aura donc pas de groupe SSp_{2n}. Désolés !

(ii) *La relation* $P \cdot (e_1, \ldots, e_{2n}) = (Pe_1, \ldots, Pe_{2n})$ *définit une action du groupe* $\mathrm{Sp}_{2n}(\mathbb{C})$ *sur l'ensemble des bases symplectiques.*

(iii) *Le groupe* $\mathrm{Sp}_{2n}(\mathbb{C})$ *agit de façon simplement transitive sur l'ensemble des bases symplectiques.*

Démonstration. (i) Supposons $P \in \mathrm{Sp}_{2n}(\mathbb{C})$ et soit (e_i) une base symplectique. On en déduit immédiatement : $\omega(Pe_i, Pe_j) = \omega(e_i, e_j)$ pour tous i dans $[1, n]$ et j dans $[1, 2n]$, puis que l'égalité est valable pour tous i et j dans $[1, 2n]$, en remarquant que ω est antisymétrique. L'automorphisme P respecte la forme bilinéaire ω sur une base, donc sur tout l'espace.

Réciproquement, si P envoie $\mathbf{e}$ sur une base symplectique, alors pour tous i et j, on a : $\omega(Pe_i, Pe_j) = \omega(e_i, e_j)$. Ainsi, P préserve ω, c'est-à-dire que P appartient à $\mathrm{Sp}_{2n}(\mathbb{C})$.

(ii) Clair par ce qui précède.

(iii) Comme le groupe linéaire agit de façon simplement transitive sur les bases, il suffit de montrer que l'action de $\mathrm{Sp}_{2n}(\mathbb{C})$ est transitive sur les bases symplectiques, ce qui résulte du premier point. □

Nous avons donc obtenu un critère géométrique pour qu'un automorphisme soit dans $\mathrm{Sp}_{2n}(\mathbb{C})$. La proposition qui suit est aussi très attendue. Il s'agit d'un résultat de type « base incomplète ».

1.3. Proposition. *Toute famille libre* $(e_1, e_2, \ldots, e_p, e_{n+1}, e_{n+2}, \ldots, e_{n+p})$, *où* p *est compris entre* 1 *et* n, *telle que*

$$\forall i \in \{1, \ldots, p\},\ \forall j \in \{1, \ldots, p\} \cup \{n+1, \ldots, n+p\}, \quad \omega(e_i, e_j) = -\delta_{i+n,j},$$

peut être complétée en une base symplectique de $\mathbb{C}^{2n}$.

Une telle famille libre pourra être appelée *système symplectique.*

Démonstration. Si $p = n$, tout va bien. Si $p < n$, il suffit de montrer que l'on peut compléter notre système symplectique de taille $2p$ en un système symplectique de taille $2p + 2$.

Soit F_p le sous-espace engendré par la famille $\langle e_1, \ldots, e_p \rangle$. L'orthogonal $F_p^{\perp\omega}$ de F_p pour ω vérifie, d'une part, $\dim F_p^{\perp\omega} = 2n - p$, car ω est non dégénérée, et, d'autre part, $F_p \subset F_p^{\perp\omega}$. L'hypothèse $p < n$ implique que l'inclusion est stricte. Soit donc e_{p+1} un vecteur de $F_p^{\perp\omega} \setminus F_p$.

On vérifie que la famille $(e_1, e_2, \ldots, e_p, e_{p+1}, e_{n+1}, e_{n+2}, \ldots, e_{n+p})$ est encore libre. En effet, une relation $\sum_i \lambda_i e_i = 0$ implique, en appliquant $\omega(e_j, ?)$, $1 \leqslant j \leqslant n$, que $\lambda_{j+n} = 0$. En remarquant que par construction $(e_1, e_2, \ldots, e_p, e_{p+1})$ est libre, on obtient bien l'assertion voulue.

Par un argument de dimension, il existe u dans

$$\langle e_1,\dots,e_p,e_{n+1},e_{n+2},\dots,e_{n+p}\rangle^{\perp_\omega} \setminus \langle e_1,\dots,e_p,e_{p+1},e_{n+1},e_{n+2},\dots,e_{n+p}\rangle^{\perp_\omega},$$

ce qui assure que $\omega(e_{p+1},u)$ est non nul. Donc, en prenant e_{n+p+1} de sorte à avoir $\omega(e_{p+1},u)\,e_{n+p+1}=u$, on règle notre affaire. □

1.4. Groupe compact symplectique et bases symplectiques orthogonales

Pour l'instant, le groupe $\mathrm{Sp}_{2n}(\mathbb{C})$ est clairement fermé comme image réciproque d'un fermé par une application continue. Mais est-il compact ? connexe ? simplement connexe ? Parmi les techniques pour l'étude de la topologie d'un groupe, nous avons vu l'efficacité redoutable de la décomposition polaire. C'est une raison suffisamment convaincante pour introduire le groupe compact symplectique $\mathrm{Sp}(n)$. Encore une fois, nous nous contentons lâchement de nous aligner avec la majorité des spécialistes des groupes symplectiques, en particulier ceux que nous croisons régulièrement dans les couloirs du labo. Il pourra donc paraître curieux, aux yeux du néophyte[3], de poser,

$$\mathrm{Sp}(n)=\mathrm{U}(2n)\cap\mathrm{Sp}_{2n}(\mathbb{C}),$$

où $\mathrm{U}(2n)$ désigne, rappelons-le, le groupe unitaire. Comme on peut s'y attendre, on verra que ce groupe constitue la partie compacte de la décomposition polaire de $\mathrm{Sp}_{2n}(\mathbb{C})$.

Encore une fois, $\mathrm{Sp}(n)$ est stable par transposition et par $*$.

On peut tout de suite fournir un critère simple d'appartenance à $\mathrm{Sp}(n)$.

1.5. Lemme. *Soit P dans $\mathrm{Sp}_{2n}(\mathbb{C})$. Alors, $P\in\mathrm{Sp}(n)\Leftrightarrow PJ=J\overline{P}$.*

Démonstration. On dit juste que si ${}^tPJP=J$, alors

$$\overline{{}^tP}P=\mathrm{Id}\Leftrightarrow PJ=J\overline{P},$$

ce qui se vérifie facilement. □

La première étape pour l'étude de ce groupe est de l'interpréter géométriquement, chose que nous allons faire à l'aide de la notion de base orthonormée symplectique. On munit l'espace $\mathbb{C}^{2n}$ de sa structure hermitienne canonique $\langle\cdot,\cdot\rangle$, préservée par le groupe unitaire U_{2n}. Notons que J est dans U_{2n} (et dans $\mathrm{O}(2n)$) puisque $J^*J=-J^2=\mathrm{Id}$.

[3]Une explication lumineuse pour cette notation sera apportée au moment de la réalisation quaternionique de ce groupe, voir remarque 1.13.

1.6. Définition. On appellera *base orthonormée symplectique* toute base orthonormée (pour $\langle \cdot, \cdot \rangle$)

$$\mathbf{e} = (e_1, e_2, \ldots, e_n, e_{n+1}, e_{n+2}, \ldots, e_{2n})$$

telle que

$$e_{n+i} = -J\overline{e_i} \qquad \forall 1 \leqslant i \leqslant n.$$

Notons que la base canonique de $\mathbb{C}^{2n}$ est orthonormée symplectique.

Il est sain de se poser la question « une base orthonormée symplectique est-elle orthonormée *et* symplectique ? » Et réciproquement, « si une base est orthonormée *et* symplectique, est-elle orthonormée symplectique ? » Et la réponse a intérêt à être oui sous peine de confusion totale dans la terminologie. Nous laissons le lecteur montrer que c'est bien le cas en se référant à la proposition suivante (en fait, le (i) suffit), qui est un copier-coller (au sens propre) de la proposition 1.2.

1.7. Proposition

(i) *Soit* $\mathbf{e}$ *une base orthonormée symplectique de* $\mathbb{C}^{2n}$. *Alors, un endomorphisme* U *de* $\mathbb{C}^{2n}$ *est dans* $\mathrm{Sp}(n)$ *si et seulement si* U *envoie* $\mathbf{e}$ *sur une base orthonormée symplectique.*

(ii) *La relation* $U \cdot (e_1, \ldots, e_{2n}) = (Ue_1, \ldots, Ue_{2n})$ *définit une action du groupe* $\mathrm{Sp}(n)$ *sur l'ensemble des bases symplectiques.*

(iii) *Par cette action, le groupe* $\mathrm{Sp}(n)$ *agit de façon simplement transitive sur l'ensemble des bases orthonormées symplectiques.*

Démonstration. (i) « Seulement si ». On suppose que U est dans $\mathrm{Sp}(n)$. Alors, l'image de $\mathbf{e}$ est orthonormée, car $U \in U_n$ et de plus, par le lemme 1.5, on a pour tout $1 \leqslant i \leqslant n$

$$Ue_{n+i} = -UJ\overline{e_i} = -J\overline{U}\overline{e_i} = -J\overline{Ue_i}.$$

Cela prouve que la base image est orthonormée symplectique.

« Si ». Par la proposition 1.2 (i), il suffit de voir qu'une base orthonormée symplectique est orthonormée et symplectique. Elle est orthonormée par définition, et symplectique par un petit calcul : pour $i \in \{1, \ldots, n\}$ et $j \in \{1, \ldots, 2n\}$, on a

$$\omega(e_i, e_j) = \langle \overline{e}_i, Je_j \rangle = \langle -J\overline{e}_i, e_j \rangle = \langle e_{n+i}, e_j \rangle = -\delta_{i+n,j}.$$

Les deux assertions (ii) et (iii) sont alors assez clairement analogues à la preuve de la proposition 1.2. □

Les propriétés topologiques de $\mathrm{Sp}(n)$ vont principalement résulter de l'étude de la réduction de $U \in \mathrm{Sp}(n)$. Commençons par un lemme de type « base incomplète », adapté à la situation.

1.8. Lemme. *Soit $p \leqslant n$ et soit*

$$\mathbf{s} = (e_1, e_2, \ldots, e_p, e_{n+1}, e_{n+2}, \ldots, e_{n+p})$$

une famille orthonormée telle que

$$\forall 1 \leqslant i \leqslant p, \quad e_{n+i} = -J\overline{e_i}.$$

Soit F le sous-espace engendré par $\mathbf{s}$ *et soit $F^\perp$ son orthogonal pour la forme hermitienne. Alors, $X \in F^\perp \iff -J\overline{X} \in F^\perp$.*

De plus, le système $\mathbf{s}$ *peut être complété en une base orthonormée symplectique.*

Démonstration. Montrons l'implication $\Rightarrow$. Si $X \in F^\perp$, alors $\langle e_i, X\rangle = 0$, pour $1 \leqslant i \leqslant p$, et donc, comme J est unitaire,

$$0 = \langle \overline{e_i}, \overline{X}\rangle = \langle J\overline{e_i}, J\overline{X}\rangle = \langle e_{n+i}, -J\overline{X}\rangle .$$

D'autre part,

$$\langle e_i, -J\overline{X}\rangle = \langle Je_i, -J^2\overline{X}\rangle = \langle -\overline{e}_{n+i}, \overline{X}\rangle = -\overline{\langle e_{n+i}, X\rangle} = 0 .$$

La réciproque en résulte puisque $J^2 = -\mathrm{I}_{2n}$.

La dernière assertion résulte alors d'une récurrence sur p. □

1.9. Proposition. *Soit $U \in \mathscr{M}_n(\mathbb{C})$. Alors, $U \in \mathrm{Sp}(n)$ si et seulement si U est $\mathrm{Sp}(n)$-semblable à une matrice diagonale de la forme*

$$U' = \left(\begin{array}{cc|cc} e^{i\theta_1} & & & \\ & \ddots & & 0 \\ & & e^{i\theta_n} & \\ \hline & & e^{-i\theta_1} & \\ 0 & & & \ddots \\ & & & e^{-i\theta_n} \end{array}\right).$$

Démonstration. La partie « si » est claire, car $U' \in \mathrm{Sp}_{2n}(\mathbb{C}) \cap U_n = \mathrm{Sp}(n)$ et $\mathrm{Sp}(n)$ est un groupe.

Montrons « seulement si ». Fixons donc U dans $\mathrm{Sp}(n)$.

On énonce d'abord le lemme suivant, qui découle directement du lemme 1.5.

Lemme. *Si v est un vecteur propre de valeur propre λ pour $U \in \mathrm{Sp}(n)$, alors $-J\overline{v}$ est un vecteur propre de valeur propre $\overline{\lambda}$ pour U.*

On va construire alors une base orthonormée symplectique $(e_1, \ldots, e_{2n})$ constituée de vecteurs propres. La matrice de passage qui envoie la base canonique (orthonormée symplectique) sur une base de vecteurs propres sera alors dans $\mathrm{Sp}(n)$ par la proposition précédente.

Soit donc e_1 un vecteur propre pour U. Comme $U \in U_n$, la valeur propre correspondante est de la forme $e^{i\theta_1}$. Soit $e_{n+1} = -Je_1$, qui est par le lemme ci-dessus un vecteur propre pour la valeur propre $e^{-i\theta_1}$ et qui est orthogonal à e_1. On considère le plan F_1 engendré par e_1 et e_{n+1}. Son orthogonal $F_1^\perp$ est stable par U (car U est unitaire) et donc la construction de la base voulue se fait par une récurrence classique en utilisant le lemme 1.8. □

1.10. Remarque. Par conséquent, l'espace des orbites pour la conjugaison de $\mathrm{Sp}(n)$ sur lui-même est homéomorphe à $(\mathbb{R}/2\pi\mathbb{R})^n/\mathfrak{S}_n$, résultat que l'on pourra comparer à [H2G2, théorème III-1.1].

La connexité de $\mathrm{Sp}(n)$, préliminaire de la connexité de $\mathrm{Sp}_{2n}(\mathbb{C})$, en résulte.

1.11. Corollaire. *Le groupe* $\mathrm{Sp}(n)$ *est un sous-groupe compact et connexe par arcs de* $\mathrm{SL}_{2n}(\mathbb{C})$.

Démonstration. On a bien un sous-groupe de $\mathrm{SL}_{2n}(\mathbb{C})$ par la proposition 1.9. La compacité est claire comme intersection du compact U_n et du fermé $\mathrm{Sp}_{2n}(\mathbb{C})$ de $\mathscr{M}_{2n}(\mathbb{C})$.

Pour la connexité par arcs, on prouve que pour tout P, il existe un arc continu reliant P et Id dans $\mathrm{Sp}(n)$. Pour tout t de $[0,1]$, on pose

$$U'(t) = \left(\begin{array}{ccc|ccc} e^{(1-t)i\theta_1} & & & & & \\ & \ddots & & & 0 & \\ & & e^{(1-t)i\theta_n} & & & \\ \hline & & & e^{-(1-t)i\theta_1} & & \\ & 0 & & & \ddots & \\ & & & & & e^{-(1-t)i\theta_n} \end{array}\right),$$

où $U = PU'P^{-1}$, $P \in \mathrm{Sp}(n)$ étant la matrice de passage dans la proposition 1.9. On vérifie que $t \mapsto PU'(t)P^{-1}$ fournit un chemin idoine. □

On en déduit également le centre de $\mathrm{Sp}(n)$.

1.12. Corollaire. *Le centre de* $\mathrm{Sp}(n)$ *est donné par* $\{\pm \mathrm{Id}\}$.

Démonstration. Par [H2G2, lemme I-A.1.23], il suffit de montrer que toute droite de $\mathbb{C}^{2n}$ peut être réalisée comme droite propre d'un élément de $\mathrm{Sp}(n)$. En effet, cela implique que le centre est constitué des matrices scalaires de $\mathrm{Sp}(n)$. Or, on peut voir que toute matrice scalaire de $\mathrm{Sp}_{2n}(\mathbb{C})$ est égale à $\pm \mathrm{Id}$.

Soit donc D une droite de $\mathbb{C}^{2n}$, engendrée par un vecteur e_1 unitaire. Par le lemme 1.8, on peut compléter la famille orthonormée $(e_1, -J\bar{e}_1 = e_{n+1})$ en

une base orthonormée symplectique $\mathbf{e} = (e_1, e_2, \dots, e_{2n})$. Il suffit de choisir un endomorphisme diagonal de valeurs propres distinctes

$$\left(e^{i\theta_1}, e^{i\theta_2}, \dots, e^{i\theta_n}, e^{-i\theta_1}, \dots, e^{-i\theta_n}\right)$$

dans la base $\mathbf{e}$, pour obtenir l'élément de $\mathrm{Sp}(n)$ voulu. □

1.13. Remarque. Pour clore ce passage obligé sur le groupe $\mathrm{Sp}(n)$, il est temps de revenir sur un peu de terminologie. Le groupe compact symplectique est aussi appelé groupe symplectique quaternionique. L'explication est simple. On munit l'espace $\mathbb{H}^n$ du produit quaternionique

$$(U, V) = \sum\nolimits_{i=1}^{n} u_i \overline{v_i} \in \mathbb{H}, \text{ où } U = (u_1, \dots, u_n), V = (v_1, \dots, v_n) \in \mathbb{H}^n,$$

et l'on identifie $\mathbb{H}$ à $\mathbb{C}^2$ en associant $u = u' + ju'' \in \mathbb{H}$ à $(u', u'') \in \mathbb{C}^2$, puis $\mathbb{H}^n$ à $\mathbb{C}^{2n}$. Alors, un simple calcul montre que pour V et W dans $\mathbb{H}^n$:

$$(V, W) = \langle V, W\rangle + \omega(V, W)\, j,$$

où $\langle \cdot, \cdot \rangle$ (resp. $\omega(\cdot, \cdot)$) est la forme hermitienne canonique (resp. la forme symplectique canonique) de $\mathbb{C}^{2n}$. Le groupe $\mathrm{O}(n, \mathbb{H})$ des $\mathbb{C}$-morphimes de $\mathbb{H}^2$ qui respectent $(\cdot, \cdot)$ est ainsi canoniquement isomorphe à $\mathrm{U}_n \cap \mathrm{Sp}_{2n}(\mathbb{C}) = \mathrm{Sp}(n)$.

Voici donc une explication lumineuse pour ceux qui trouveraient curieuse la notation $\mathrm{Sp}(n)$ pour un sous-groupe de $\mathrm{GL}_{2n}(\mathbb{C})$. Mieux, en traduisant scrupuleusement la preuve de l'homéomorphisme $\mathrm{O}_n(\mathbb{R})/\mathrm{O}_{n-1}(\mathbb{R}) \simeq \mathbf{S}^{n-1}$ dans [H2G2, proposition II-4.1.6], on obtient un homéomorphisme $\mathrm{Sp}(n)/\mathrm{Sp}(n-1) \simeq \mathbf{S}^{4n-1}$. Cela implique par récurrence la simple connexité de $\mathrm{Sp}(n)$ à partir de la simple connexité de la sphère $\mathbf{S}^{4n-1}$. On trouve les détails dans [H2G2, exercice VII-C.4].

1.14. Matrices hermitiennes définies positives de $\mathrm{Sp}_{2n}(\mathbb{C})$

Dans la logique impitoyable de la décomposition polaire, on se doit d'étudier l'ensemble des matrices symplectiques hermitiennes définies positives. L'étude sera très analogue à celle de $\mathrm{Sp}(n)$: caractérisation algébrique, réduction, et enfin propriétés topologiques. Peut-être en plus expéditif...

On considère donc l'ensemble des matrices hermitiennes définies positives *et* symplectiques :

$$\mathscr{H}^{\omega}(n) = \mathscr{H}_{2n}^{++} \cap \mathrm{Sp}_{2n}(\mathbb{C}).$$

Voici une première caractérisation immédiate.

1.15. Lemme. *Soit $H \in \mathscr{H}_{2n}^{++}$. On a l'équivalence entre les assertions :*

(i) $H \in \mathrm{Sp}_{2n}(\mathbb{C})$;

(ii) $HJ\overline{H} = J$.

On en déduit le lemme de réduction suivant (on rappelle que les valeurs propres d'une matrice hermitienne définie positive ne sauraient être nulles).

1.16. Lemme. *Soit $H \in \mathscr{H}^{\omega}(n)$. Si v est un vecteur propre de H de valeur propre λ, alors $-J\overline{v}$ est un vecteur propre de H de valeur propre $1/\lambda$.*

La proposition suivante est une version hermitienne de la proposition 1.9 et l'adaptation de la preuve sera laissée au lecteur. Parmi les outils, seul change le lemme qui précède.

1.17. Proposition. *Soit $H \in \mathscr{M}_{2n}(\mathbb{C})$. Alors, $H \in \mathscr{H}^{\omega}(n)$ si et seulement si H est $\mathrm{Sp}(n)$-semblable à une matrice diagonale de la forme*

$$H' = \left(\begin{array}{cc|cc} \lambda_1 & & & \\ & & & 0 \\ & \lambda_n & & \\ \hline & & \frac{1}{\lambda_1} & \\ & 0 & & \\ & & & \frac{1}{\lambda_n} \end{array}\right),$$

où les λ_j sont des réels strictement positifs.

Il est temps de récolter les informations voulues sur $\mathscr{H}^{\omega}(n)$.

1.18. Corollaire. *On a les propriétés suivantes.*

(i) *L'espace topologique $\mathscr{H}^{\omega}(n)$ est connexe par arcs,*

(ii) *L'application $\mathscr{H}^{\omega}(n) \to \mathscr{H}^{\omega}(n)$, $H \mapsto H^2$ est un homéomorphisme.*

Démonstration. La première assertion découle de la proposition 1.17 et de la connexité par arcs de $\mathbb{R}^{+*}$: il suffit de réduire une matrice H comme dans la proposition précédente et de créer des chemins de $\mathbb{R}^{+*}$ qui connectent λ_j à 1 dans la matrice H', par exemple en remplaçant λ_j par $\exp(t \ln \lambda_j)$ pour $t \in [0,1]$).

La seconde provient également de la proposition et du fait que $H \mapsto H^2$ réalise un homéomorphisme de $\mathscr{H}_{2n}^{++}$ dans lui-même, ce que l'on sait déjà par [H2G2, proposition VI-2.3 (ii)]. □

On peut montrer ce corollaire de façon plus simple, et même mieux : obtenir un raffinement de ce corollaire de façon plus simple. L'utilisation de l'exponentielle est providentielle.

1.19. Proposition. *Soit H une matrice hermitienne de $\mathscr{H}_{2n}$. Les conditions suivantes sont équivalentes.*

(i) $\exp(H) \in \mathscr{H}^{\omega}(n)$;

(ii) ${}^tHJ + JH = 0$;

(iii) *la matrice H s'écrit par blocs $n \times n$ sous la forme*

$$H = \begin{pmatrix} A & \overline{B} \\ B & -\overline{A} \end{pmatrix},$$

où A est une matrice hermitienne et B une matrice symétrique.

Démonstration. L'exponentielle réalise un homéomorphisme entre l'espace réel des matrices hermitiennes $\mathscr{H}_{2n}$ et le cône des matrices définies positives $\mathscr{H}_{2n}^{++}$ ([H2G2, proposition VI-2.3 (ii)]). Pour un élément H de $\mathscr{H}_{2n}$, l'exponentielle $\exp(H)$ appartient à $\mathscr{H}^{\omega}(n)$ si et seulement si $\exp(H)$ appartient à $\mathrm{Sp}_{2n}(\mathbb{C})$, c'est-à-dire si H satisfait à ${}^t\exp(H)J\exp(H) = J$. On peut écrire cette relation $\exp(-H) = \exp(J^{-1}\,{}^tHJ)$ en utilisant les propriétés classiques de l'exponentielle, voir par exemple [H2G2, proposition VI-2.1]. Ainsi, l'assertion (i) équivaut à la condition : $-H = J^{-1}\,{}^tHJ$.

L'équivalence avec l'assertion (iii) s'obtient en décomposant H en quatre blocs carrés et en écrivant les relations $H^* = H$ et $-H = J^{-1}\,{}^tHJ$ en termes de ces blocs. □

Tout est désormais en place pour étudier les diverses propriétés de $\mathrm{Sp}(2n, \mathbb{C})$ via la décomposition polaire.

1.20. Proposition (Décomposition polaire du groupe symplectique) *On a un homéomorphisme de décomposition polaire*

$$\mu : \mathscr{H}^{\omega}(n) \times \mathrm{Sp}(n) \longrightarrow \mathrm{Sp}_{2n}(\mathbb{C}),$$

où μ désigne la multiplication.

Démonstration. L'application μ est bien définie, car $\mathrm{Sp}_{2n}(\mathbb{C})$ est un groupe.

D'après [H2G2, proposition VI-2.3 (ii)], la réciproque de l'opération de multiplication $\mathscr{H}_{2n}^{++} \times \mathrm{U}_{2n} \to \mathrm{GL}_{2n}(\mathbb{C})$ est également continue et est donnée par $A \mapsto HU$, où H est l'unique matrice de $\mathscr{H}_{2n}^{++}$ telle que $H^2 = AA^*$, et $U = H^{-1}A$. Il reste donc juste à montrer que la réciproque de μ est bien définie. Cela résulte du corollaire 1.18. □

Mais qu'est-ce qu'on ferait sans la décomposition polaire ?

1.21. Corollaire. *Le groupe $\mathrm{Sp}_{2n}(\mathbb{C})$ est un sous-groupe connexe de $\mathrm{SL}_{2n}(\mathbb{C})$ (et fermé).*

Démonstration. Le fait que $\mathrm{Sp}_{2n}(\mathbb{C})$ soit fermé ne fait aucun doute. Par les corollaires 1.11 et 1.18, les parties $\mathscr{H}^\omega(n)$ et $\mathrm{Sp}(n)$ sont connexes, donc leur produit $\Pi = \mathscr{H}^\omega(n) \times \mathrm{Sp}(n)$ l'est. Or, $\mathrm{Sp}_{2n}(\mathbb{C})$ est l'image du produit Π par l'application continue μ, donc $\mathrm{Sp}_{2n}(\mathbb{C})$ est connexe.

Les résultats vus précédemment sur $\mathscr{H}^\omega(n)$ et $\mathrm{Sp}(n)$ entraînent que ce sont deux parties de $\mathrm{SL}_{2n}(\mathbb{C})$. Donc, par produit matriciel, $\mathrm{Sp}_{2n}(\mathbb{C})$ est un sous-groupe de $\mathrm{SL}_{2n}(\mathbb{C})$. □

La preuve de ce corollaire est calquée sur celle du corollaire 1.12 ; elle est laissée sans inquiétude au lecteur.

1.22. Corollaire. *Le centre de* $\mathrm{Sp}_{2n}(\mathbb{C})$ *est* $\{\pm \mathrm{Id}\}$.

Voici pour terminer quelques algèbres de Lie.

1.23. Proposition. *Le groupe* $\mathrm{Sp}_{2n}(\mathbb{C})$ *est un groupe de Lie dont l'algèbre de Lie* $\mathfrak{sp}_{2n}(\mathbb{C})$ *associée est donnée par*

$$\mathfrak{sp}_{2n}(\mathbb{C}) = \big\{M \in \mathscr{M}_{2n}(\mathbb{C}),\ {}^tMJ + JM = 0_{2n}\big\}.$$

Sa dimension complexe est : $\dim_{\mathbb{C}} \mathfrak{sp}_{2n}(\mathbb{C}) = n(2n+1)$.

Le groupe $\mathrm{Sp}(n)$ *est un groupe de Lie dont l'algèbre de Lie* $\mathfrak{sp}(n)$ *associée est donnée par :*

$$\begin{aligned}\mathfrak{sp}(n) &= \mathfrak{sp}_{2n}(\mathbb{C}) \cap \mathfrak{u}_n \\ &= \big\{M \in \mathscr{M}_{2n}(\mathbb{C}),\ {}^tMJ + JM = 0_{2n},\ M^* + M = 0_{2n}\big\}.\end{aligned}$$

Sa dimension (réelle) est : $\dim_{\mathbb{R}} \mathfrak{sp}(n) = n(2n+1)$.

Démonstration. On va appliquer [H2G2, théorème IX-A.4.2], après avoir montré que l'application $\phi : \mathrm{GL}_{2n}(\mathbb{C}) \to \mathscr{A}_{2n}(\mathbb{C})$, $M \mapsto {}^tMJM$, est une submersion en tout M de $\mathrm{Sp}_{2n}(\mathbb{C})$.

Soit M dans $\mathrm{Sp}_{2n}(\mathbb{C})$ et soit X dans l'espace tangent de $\mathrm{GL}_{2n}(\mathbb{C})$ en M. Alors, ϕ est différentiable en M et sa différentielle vaut $\mathrm{d}\phi_M(X) = {}^tXJM + {}^tMJX$. Vérifions que toute matrice antisymétrique N possède un antécédent par $\mathrm{d}\phi_M$: la matrice définie par $2X = J^{-1}\,{}^tM^{-1}N$ fait l'affaire.

On voit facilement par le calcul que $M = \left(\begin{smallmatrix} A & C \\ B & D \end{smallmatrix}\right)$, où tous les blocs sont de taille $n \times n$, vérifie ${}^tMJ + JM = 0_{2n}$ si et seulement si B et C sont symétriques et $D = -{}^tA$. Ainsi, l'espace vectoriel complexe $\mathfrak{sp}_{2n}(\mathbb{C})$ est isomorphe à $\mathscr{S}_n(\mathbb{C}) \times \mathscr{S}_n(\mathbb{C}) \times \mathscr{M}_n(\mathbb{C})$. Cela entraîne le résultat sur sa dimension.

Par [H2G2, théorème IX-B.11], $\mathrm{Sp}(n)$ est un groupe de Lie dont l'algèbre de Lie $\mathfrak{sp}(n)$ est égale à $\mathfrak{sp}_{2n}(\mathbb{C}) \cap \mathfrak{u}_n$.

Cette dernière égalité provient immédiatement du fait que l'algèbre de Lie d'un sous-groupe de Lie G de $\mathrm{GL}_m(\mathbb{C})$ est le sous-espace des matrices X de $\mathscr{M}_m(\mathbb{C})$ telles que $\exp(tX) \in G$ pour tout t réel.

Par un calcul par blocs facile, on voit que l'espace vectoriel réel $\mathfrak{sp}_{2n}(\mathbb{C}) \cap \mathfrak{u}_n$ est isomorphe à $\mathscr{S}_n(\mathbb{R}) \times \mathscr{S}_n(\mathbb{R}) \times \mathscr{AH}_n$, où $\mathscr{AH}_n$ désigne l'espace réel des matrices antihermitiennes $n \times n$. Sa dimension réelle est donc $n(2n+1)$.□

1.24. Remarque. On peut s'arrêter une seconde sur le problème de l'intersection de deux sous-groupes de Lie de $\mathrm{GL}_m(\mathbb{C})$. En général, l'espace tangent en un point de l'intersection de deux sous-variétés différentielles n'est pas égal à l'intersection des espaces tangents de chacune des sous-variétés en ce point. Il est d'ailleurs toujours inclus, mais cette intersection peut être stricte (prendre par exemple l'intersection d'une courbe lisse avec sa tangente en un point). Pour l'égalité, il faut que l'intersection soit « transverse ». Dans le cadre des groupes de Lie, cette condition est automatiquement vérifiée. Cela est dû au fait, comme on peut le voir dans la preuve précédente, que c'est toujours la même fonction, l'exponentielle pour ne pas la nommer, qui réalise les cartes des sous-variétés.

1.25. Remarque. On voit également que $\mathfrak{sp}_{2n}(\mathbb{C}) \cap \mathscr{H}_n$ est isomorphe à $\mathscr{S}_n(\mathbb{R}) \times \mathscr{S}_n(\mathbb{R}) \times \mathscr{H}_n$. Sa dimension réelle est donc $n(2n+1)$. Par la proposition 1.19, l'intersection $\mathscr{H}_n^{++} \cap \mathrm{Sp}_{2n}(\mathbb{C})$ est donc une sous-variété différentielle de dimension réelle $n(2n+1)$.

On peut retrouver ce résultat grâce à la décomposition polaire de $\mathrm{Sp}_{2n}(\mathbb{C})$.

1.26. Remarque. L'algèbre de Lie $\mathfrak{sp}_{2n}(\mathbb{C})$ est donc constituée des matrices A telles que ${}^tA = -JAJ^{-1}$, ce qui implique, en prenant la trace, l'inclusion $\mathfrak{sp}_{2n}(\mathbb{C})$ dans l'algèbre de Lie $\mathfrak{sl}(2n, \mathbb{C})$ des matrices de trace nulle. Cela conforte le fait que $\mathrm{Sp}_{2n}(\mathbb{C}) \subset \mathrm{SL}_{2n}(\mathbb{C})$, voir corollaire 1.21. En revanche, cela ne saurait donner une preuve indépendante que $\mathrm{Sp}_{2n}(\mathbb{C}) \subset \mathrm{SL}_{2n}(\mathbb{C})$, sauf si l'on sait à l'avance que $\mathrm{Sp}_{2n}(\mathbb{C})$ est connexe. Or, les deux propriétés ont été prouvées dans la même foulée.

2. Correspondances de Klein

Sur trois exemples, nous allons voir deux aspects d'une même correspondance : un aspect se situe dans le registre des groupes, l'autre, sur le plan de la géométrie. Ces correspondances sont (assez) communément appelées correspondances de Klein. Pour le point de vue des groupes, on montrera des isomorphismes exceptionnels, sur le corps $\mathbb{C}$, afin d'utiliser l'apport précieux de la géométrie différentielle. En revanche, le versant géométrique se fera sur un corps quelconque de caractéristique différente de 2. Le lien

entre la version groupiste et la version géométrique (disons, sur $\mathbb{C}$) est la suivante : dans les trois cas, nous avons un isomorphisme (exceptionnel) entre deux groupes, disons G et G', qui agissent respectivement (de façon naturelle) sur deux ensembles X et X', eux-mêmes en bijection, de sorte que la bijection induite entre $G \times X$ et $G' \times X'$ commute aux actions. Pour le point de vue des groupes (mais les autres points de vue sont les bienvenus), la bijection de X vers X' sera interprétée comme un versant géométrique de l'isomorphisme entre G et G'.

2.1. Isomorphisme $\mathrm{PSL}_2(\mathbb{C}) \simeq \mathrm{SO}_3(\mathbb{C})$ et versant géométrique

Comme constaté dans [H2G2, proposition IX-2.1], on a l'isomorphisme exceptionnel $\mathrm{PSL}_2(\mathbb{C}) \simeq \mathrm{SO}_3(\mathbb{C})$. Pour mémoire, il peut être obtenu en faisant agir $\mathrm{SL}_2(\mathbb{C})$ sur son algèbre de Lie $\mathfrak{sl}_2(\mathbb{C})$ par conjugaison, action qui laisse stable le déterminant, lequel est une forme quadratique non dégénérée sur un espace de dimension 3.

2.1.1. Versant géométrique de $\mathrm{PSL}_2(\mathbb{C}) \simeq \mathrm{SO}_3(\mathbb{C})$ sur un corps $\mathbb{K}$

Voici une petite digression géométrique. Le résultat que nous allons montrer peut s'énoncer ainsi : il existe une bijection naturelle entre $\mathbb{P}^1(\mathbb{K})$ et une quadrique de $\mathbb{P}^2(\mathbb{K})$. En particulier, si $\mathbb{K} = \mathbb{C}$, on sait que $\mathrm{PSL}_2(\mathbb{C})$ agit naturellement sur $\mathbb{P}^1(\mathbb{C})$ et que $\mathrm{SO}_3(\mathbb{C})$ agit naturellement sur une quadrique projective de $\mathbb{P}^2(\mathbb{C})$, nommément $x^2 + y^2 + z^2 = 0$. Ce que dit la proposition 2.2, c'est qu'il existe une bijection entre $\mathbb{P}^1(\mathbb{C})$ et la quadrique de $\mathbb{P}^2(\mathbb{C})$ telle que l'isomorphisme exceptionnel $\mathbb{P}^1(\mathbb{C}) \simeq \mathrm{SO}_3(\mathbb{C})$ fasse commuter ces deux actions. Ainsi, cette bijection peut être vue comme un versant géométrique de cet isomorphisme exceptionnel.

Soit Q la quadrique projective d'équation $\det(A) = 0$ dans $\mathbb{P}\mathfrak{sl}_2$ (ce qui a un sens puisque det est une forme quadratique sur $\mathfrak{sl}_2$). On a déjà noté précédemment que cela est équivalent à dire, par le théorème de Cayley-Hamilton, que A est non nulle et nilpotente d'indice de nilpotence 2. On définit les applications α et β suivantes :

$$\alpha : \mathbb{P}^1 \to Q,\ D = \langle x \rangle \mapsto \mathbb{K}(x\,{}^t x'), \quad \beta : Q \to \mathbb{P}^1,\ A \mapsto \operatorname{im} A,$$

où x est un générateur de la droite D et x' un générateur de $D^\perp$ pour la forme bilinéaire symétrique canonique de $\mathbb{K}^2$ (on confondra ici vecteur et coordonnées). On peut aussi préférer la formule en coordonnées homogènes

$$\alpha\big((a : b)\big) = \begin{pmatrix} ab & -a^2 \\ b^2 & -ab \end{pmatrix}, \text{ pour } a, b \in \mathbb{C}.$$

2.2. Proposition. *Les applications α et β sont bien définies et réalisent deux bijections réciproques entre la droite projective $\mathbb{P}^1(\mathbb{K})$ et la quadrique projective Q. De plus, pour les actions naturelles, on a pour tout P et P' de $\mathrm{SL}_2(\mathbb{K})$, $F \in \mathbb{P}^1$, la relation : $\alpha(P \cdot F) = P\alpha(F)P^{-1}$.*

Démonstration. Montrons que α et β sont bien définies. En effet, si x est un générateur de D (vu comme un vecteur colonne), il est non nul et défini de façon unique à un scalaire près, ainsi qu'un orthogonal x'. La matrice $x\,{}^t x'$ (c'est le produit d'un vecteur colonne par un vecteur ligne, il s'agit donc ici d'une matrice carrée de taille 2) est donc bien non nulle et définie de façon unique à scalaire près. De plus, la pseudo-associativité de la multiplication matricielle assure que $(x\,{}^t x')^2 = x({}^t x' x)\,{}^t x' = 0$ et donc que $x\,{}^t x'$ est bien nilpotente (d'indice 2). Ainsi, $x\,{}^t x'$ est de trace et de déterminant nul. Il est clair que β est bien définie, car $\mathrm{im}(A)$ est bien de dimension 1 et ne dépend pas de la matrice choisie sur la droite engendrée par A.

On a par construction : $\beta\alpha = \mathrm{Id}$. Reste donc à montrer que α est surjective. Pour cela, supposons A dans Q, à scalaire près. Alors, A est de rang 1 et donc $A = x\,{}^t y$ pour deux éléments x et y de $\mathbb{K}^2$. On a vu que $A^2 = 0$, donc $\mathrm{im}\,A = \ker A$ (inclusion claire et égalité par dimension). Or,

$$\ker A = (\mathrm{im}\,{}^t A)^\perp = (\mathrm{im}\, y\,{}^t x)^\perp = \langle y\rangle^\perp.$$

On en déduit : $\langle y\rangle = (\ker A)^\perp = (\mathrm{im}\,A)^\perp = \langle x\rangle^\perp$, ce qui donne la surjectivité. La dernière assertion est immédiate si l'on remarque que

$$\mathrm{im}\big(P(x\,{}^t x')P^{-1}\big) = \mathrm{im}\big((Px)\,{}^t({}^t P^{-1} x')\big) = \langle Px\rangle = P\langle x\rangle\,. \qquad \square$$

2.3. Remarque. Pour une généralisation de l'application α, voir le *plongement de Veronese*, on pourra se référer à l'excellent livre [31] de William Fulton et Joe Harris.

2.4. Isomorphisme $\mathbf{SL_2(\mathbb{C})\times SL_2(\mathbb{C})/\{(I_2, I_2), (-I_2, -I_2)\} \simeq SO_4(\mathbb{C})}$ et versant géométrique

Montrons tout d'abord en exercice l'isomorphisme exceptionnel annoncé, qui s'apparente à cet autre, non moins exceptionnel, prouvé dans [H2G2, proposition VII-4.1].

2.5. Exercice. *On se propose de montrer que l'action de* $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$ *sur* $\mathscr{M}_2(\mathbb{C})$ *donnée par* $(P, P') \cdot A = PAP'^{-1}$ *fournit un isomorphisme de groupes*

$$\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})/\{(\mathrm{I}_2, \mathrm{I}_2), (-\mathrm{I}_2, -\mathrm{I}_2)\} \simeq \mathrm{SO}_4(\mathbb{C}).$$

1. *Soit* ϕ *le morphisme associé à l'action. Sachant que* $\det PAP'^{-1} = \det A$, *montrer que* $\mathrm{im}\,\phi \subset \mathrm{SO}(\det) \simeq \mathrm{SO}_4(\mathbb{C})$.

   Le déterminant est une forme quadratique non dégénérée sur $\mathscr{M}_2(\mathbb{C})$, ce qui donne l'inclusion dans $\mathrm{O}(\det) \simeq \mathrm{O}_4(\mathbb{C})$. L'inclusion dans $\mathrm{SO}(\det)$ provient de façon classique de la connexité de $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$.

2. *On veut montrer que* $\ker\phi = \{(\lambda\,\mathrm{Id}, \lambda^{-1}\,\mathrm{Id}),\ \lambda = \pm 1\}$.
   (a) *Montrer l'inclusion inverse (de droite à gauche).*
   (b) *Soit* $(P, P') \in \ker\phi$. *Supposons, par l'absurde, que* P' *envoie (par abus de langage) une droite* D *sur une droite* D' *distincte de* D. *Montrer que l'on peut trouver une matrice* A *telle que* $AD = D$ *et* $AD' = 0$. *Utiliser l'identité* $PAP'^{-1} = A$ *pour trouver une contradiction, et conclure que* P' *est une homothétie.*
   (c) *Montrer que si* $(P, P') \in \ker\phi$, *alors* $({}^tP', {}^tP) \in \ker\phi$. *Conclure.*
3. *Montrer la surjectivité en utilisant la théorie de Lie (comme, par exemple, dans la preuve de [H2G2, proposition IX-2.1]).*
4. *On se propose de généraliser ce résultat à d'autres corps.*
   (a) *Montrer que, pour un corps quelconque* $\mathbb{K}$, *on a :*
   $$\mathrm{SL}_2(\mathbb{K}) \times \mathrm{SL}_2(\mathbb{K})/\{\pm 1\} \hookrightarrow \mathrm{O}(q),$$
   où q *est la forme quadratique sur* $\mathbb{K}^4$ *donnée par :* $q = x_1x_4 - x_2x_3$.
   (b) *Montrer que si* $\mathbb{K} = \mathbb{R}$, *alors* $\mathrm{im}\,\phi = \mathrm{SO}_0(2,2)$, *et, en utilisant le théorème IV-2.1, que si* $\mathbb{K}$ *est un corps fini de caractéristique différente de* 2, *alors* $\mathrm{im}\,\phi$ *est un sous-groupe d'indice* 4 *dans* $\mathrm{O}_4(\mathbb{K})$.

2.5.1. Versant géométrique de $\mathbf{SL_2(\mathbb{C})\times SL_2(\mathbb{C})/\{\pm(I_2,I_2)\}\simeq SO_4(\mathbb{C})}$ sur un corps $\mathbb{K}$

En lien direct avec l'exercice précédent (mais que nous allons traiter indépendamment), nous démontrerons la propriété suivante : pour tout corps $\mathbb{K}$, il existe une quadrique projective de $\mathbb{P}^3$ en bijection naturelle[4] avec $\mathbb{P}^1 \times \mathbb{P}^1$. Pour cela, il suffit d'identifier l'espace projectif $\mathbb{P}^3$ avec $\mathbb{P}\mathscr{M}_2(\mathbb{K})$. Soit Q la quadrique projective d'équation $\det(A) = 0$ dans $\mathbb{P}\mathscr{M}_2(\mathbb{K})$ (ce qui a un sens puisque le déterminant est homogène). On note que cela est équivalent à dire que A est non nulle et de rang 1. On définit les applications α et β suivantes :

$$\alpha : \mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow Q, \quad \big((x:y),(x':y')\big) \longmapsto \mathbb{K}\begin{pmatrix} xy' & -xx' \\ yy' & -yx' \end{pmatrix},$$

$$\beta : Q \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1, \quad A \longmapsto (\mathrm{im}\,A, \ker A).$$

2.6. Proposition. *Les applications* α *et* β *sont bien définies et réalisent deux bijections réciproques entre la droite projective* $\mathbb{P}^1 \times \mathbb{P}^1$ *et la quadrique projective* Q. *De plus, pour les actions naturelles, on a pour tout* P *de* SL_2 *la relation :*

$$\alpha\big((P\cdot D, P'\cdot D')\big) = P\alpha\big((D,D')\big)P'^{-1}.$$

[4] On a également, sur $\mathbb{C}$, une propriété de compatibilité des actions naturelles, via l'isomorphisme exceptionnel $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})/\{(\mathrm{I}_2,\mathrm{I}_2),(-\mathrm{I}_2,-\mathrm{I}_2)\} \simeq \mathrm{SO}_4(\mathbb{C})$, comme dans 2.1.1.

Démonstration. Montrons que α et β sont bien définies. Pour α, il suffit de voir que la matrice ci-dessus n'est jamais nulle, qu'elle est indépendante des représentants respectifs de $(x : y)$ et $(x' : y')$, et qu'elle est de déterminant nul, ce qui ne devrait poser de problème à personne à ce stade. De même, l'application β est bien définie puisque $\operatorname{im}(A)$ et $\ker(A)$ ne changent pas lorsque l'on multiplie A par un scalaire non nul.

On a immédiatement : $\beta\alpha = \mathrm{Id}_{\mathbb{P}^1\times\mathbb{P}^1}$. Il reste alors à montrer que β est injective, c'est-à-dire qu'une matrice 2×2 de rang 1 est déterminée à scalaire près par son image et son noyau. Soit X une matrice d'image engendrée par u non nul et de noyau engendré par v non nul. Alors, $X = u\,{}^t y$ pour un y et ${}^t X = v'\,{}^t x$, où v' est un orthogonal de v, étant donné que $\operatorname{im}{}^t X = (\ker X)^\perp$. On déduit donc de ces deux égalités que $X = \lambda u\,{}^t v'$, ce qui prouve l'assertion.

Comme $\operatorname{im} PAP'^{-1} = P \operatorname{im} A$ et $\ker PAP'^{-1} = P' \ker A$, nous avons la compatibilité de β, et donc de α avec l'action de $\mathrm{SL}_2(\mathbb{K})$ comme désiré. □

2.7. Remarque. L'application α de la proposition se généralise en beauté : c'est le cas particulier du *plongement de Segre* (exercice B.6)

$$\mathbb{P}^n(\mathbb{K}) \times \mathbb{P}^m(\mathbb{K}) \hookrightarrow \mathbb{P}^{(n+1)(m+1)-1}(\mathbb{K}),$$

qui permet de considérer le produit de deux espaces projectifs comme une quadrique dans un espace projectif[5].

2.8. Isomorphisme exceptionnel $\mathrm{SL}_4(\mathbb{C})/\{\mathrm{Id}, -\mathrm{Id}\} \simeq \mathrm{SO}_6(\mathbb{C})$ et versant géométrique

La *correspondance de Klein* peut être vue comme une bijection (en fait pour être précis, un morphisme de variétés algébriques) entre les lignes de l'espace projectif de dimension 3 et une quadrique de l'espace projectif de dimension 5. Nous verrons cette correspondance sur $\mathbb{C}$ à travers un isomorphisme exceptionnel entre un quotient de $\mathrm{SL}_4(\mathbb{C})$ et $\mathrm{SO}_6(\mathbb{C})$, appelé parfois « groupe strasbourgeois[6] », ou mieux comme un isomorphisme entre les quotients simples $\mathrm{PSL}_4(\mathbb{C})$ et $\mathrm{PSO}_6(\mathbb{C})$. Ces résultats proviennent principalement d'une identité polynomiale valable sur $\mathbb{Z}$ et s'adaptent donc sans mal sur $\mathbb{R}$ ainsi que sur les corps finis. Le pfaffien joue ici un rôle fondamental.

Commençons donc par définir cette forme. On la définira en dimension 4, même si elle peut se définir en dimension quelconque, témoin l'exercice B.4. On considère donc l'espace $\mathscr{A}_4(\mathbb{C})$ des matrices antisymétriques de $\mathscr{M}_4(\mathbb{C})$.

[5]Le produit de deux espaces affines est clairement un espace affine. L'équivalent n'est plus vrai pour les espaces projectifs. Le plongement de Segre permet de pallier ce problème.

[6]Nous remercions au passage Claude Roger pour ses calembours et contrepèteries joyeux.

2.9. Définition. On appelle *pfaffien* la forme quadratique donnée sur $\mathscr{A}_4(\mathbb{C})$ par :

$$\mathrm{Pf} : \mathscr{A}_4(\mathbb{C}) \to \mathbb{C}, \quad A = \begin{pmatrix} 0 & -a & -b & -c \\ a & 0 & -d & -e \\ b & d & 0 & -f \\ c & e & f & 0 \end{pmatrix} \mapsto af - be + cd.$$

On vérifie, par exemple en utilisant la méthode de Gauss, que Pf est une forme quadratique non dégénérée sur $\mathscr{A}_4$ et donc, par [H2G2, théorème V-1.2 (i)], le groupe orthogonal de Pf est isomorphe à $\mathrm{O}_6(\mathbb{C})$. Dévoilons dès maintenant la formule fondamentale, valable sur $\mathbb{Z}$, sur laquelle tous les résultats vont s'articuler et qui peut se montrer sans difficulté par un calcul direct :

$$\mathrm{Pf}(A)^2 = \det(A), \ A \in \mathscr{A}_4(\mathbb{C}).$$

Autrement dit : vu comme polynôme à six indéterminées, le déterminant d'une matrice antisymétrique est un carré ! Et cela reste vrai en toute dimension (paire, pour que ce soit intéressant).

Pour ceux qui aiment ces exécutions sans sommations (!) que constituent les calculs de déterminants, notons qu'il est ici pratique de développer $\det(A)$ par rapport aux deux premières lignes (si vous ne connaissez pas le développement par rapport à deux lignes données, inventez-le, ou allez voir le théorème I-1.8 sur le développement de Laplace). Pour ceux qui ne seraient toutefois pas satisfaits par cette preuve calculatoire, notons que ce résultat, ainsi que la généralisation en toute dimension, se prouve de façon naturelle dans le cadre de la théorie des représentations des groupes semi-simples, voir par exemple le livre [31].

2.10. Proposition. *L'action de* $\mathrm{SL}_4(\mathbb{C})$ *par congruence sur* $\mathscr{A}_4(\mathbb{C})$ *fixe le pfaffien.*

Démonstration. Il suffit donc de montrer que pour tout P dans $\mathrm{SL}_4(\mathbb{C})$ et A dans $\mathscr{A}_4(C)$, on a : $\mathrm{Pf}(PA\,{}^tP) = \mathrm{Pf}(A)$. Notons que cela a un sens puisque $PA\,{}^tP$ et A sont antisymétriques.

Supposons A inversible. Comme le carré du pfaffien est le déterminant, on a : $\mathrm{Pf}(A) \neq 0$. Posons, pour $P \in \mathrm{SL}_4(\mathbb{C})$: $f(P) = \mathrm{Pf}(PA\,{}^tP)/\mathrm{Pf}(A)$. Il vient :

$$f(P)^2 = \frac{\det(PA\,{}^tP)}{\det(A)} = \det(P)^2 = 1.$$

On en déduit que f est une fonction continue (fraction rationnelle) sur $\mathrm{SL}_4(\mathbb{C})$ (lequel est connexe) et à valeur[7] dans $\{1, -1\}$. Il en résulte que f est constante et cette constante vaut $f(\mathrm{Id}) = 1$.

[7] *A posteriori*, le singulier n'est pas une faute d'orthographe.

Nous avons donc bien que $\mathrm{Pf}(PA\,{}^tP) = \mathrm{Pf}(A)$ si A est inversible. Si A ne l'est pas, on a : $\mathrm{Pf}(A) = 0$ et $\mathrm{Pf}(PA\,{}^tP) = 0 = \mathrm{Pf}(A)$. □

2.11. Exercice. *Adapter la preuve ci-dessus pour montrer que pour P matrice* quelconque *de $\mathscr{M}_4(\mathbb{C})$ et A antisymétrique, on a :* $\mathrm{Pf}(PA\,{}^tP) = \det(P)\,\mathrm{Pf}(A)$.

Notons encore que l'égalité $\mathrm{Pf}(PA\,{}^tP) = \mathrm{Pf}(A)$, $P \in \mathrm{SL}_4(\mathbb{C})$ qui a été prouvée à l'aide d'un argument topologique sur $\mathbb{C}$, est du coup valable sur $\mathbb{Z}$. Cela n'implique pas immédiatement que le résultat soit vrai sur $\mathbb{F}_p$ puisqu'il n'est pas clair *a priori*[8] qu'une matrice de $\mathrm{SL}_4(\mathbb{F}_p)$ provienne de la réduction d'une matrice de $\mathrm{SL}_4(\mathbb{Z})$. En revanche, le résultat de l'exercice précédent prouve que la proposition s'adapte sur n'importe quel corps : l'égalité polynomiale $\mathrm{Pf}(PA\,{}^tP) = \det(P)\,\mathrm{Pf}(A)$, où (P, A) est dans l'espace vectoriel $\mathscr{M}_4 \times \mathscr{A}_4$ est valable sur $\mathbb{Z}$ et donc sur tout corps, ce qui implique la généralisation voulue. Ce genre de preuve, mélangeant topologie sur $\mathbb{C}$ et polynomialité sur $\mathbb{Z}$ n'est pas sans rappeler la preuve express du théorème de Cayley-Hamilton sur tout corps, voir remarque III-D.3. Voici maintenant l'isomorphisme annoncé.

2.12. Théorème. *L'action de* $\mathrm{SL}_4(\mathbb{C})$ *sur* $\mathscr{A}_4(\mathbb{C})$ *par congruence induit un isomorphisme de groupes* $\mathrm{SL}_4(\mathbb{C})/\{\mathrm{Id}, -\mathrm{Id}\} \simeq \mathrm{SO}_6(\mathbb{C})$.

2.13. Remarque. Les groupes $\mathrm{SL}_4(\mathbb{C})/\{1, -1\}$ et $\mathrm{SO}_6(\mathbb{C})$ ne sont pas simples car leur centre est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. En revanche les quotients par leurs centres respectifs sont simples (et, bien sûr, isomorphes).

Démonstration. Comme l'action qui précède est linéaire et respecte la forme quadratique non dégénérée (donc unique à congruence près) Pf sur l'espace $\mathscr{A}_4$ de dimension 6, il vient que le morphisme ϕ de l'action envoie $\mathrm{SL}_4(\mathbb{C})$ sur $\mathrm{O}(\mathrm{Pf})$ qui est isomorphe à $\mathrm{O}_6(\mathbb{C})$, puisque Pf est non dégénérée sur $\mathbb{C}$. Par connexité de $\mathrm{SL}_4(\mathbb{C})$, et par continuité du morphisme, son image est dans la composante connexe de l'identité $\mathrm{SO}(\mathrm{Pf}) \simeq \mathrm{SO}_6(\mathbb{C})$.

Montrons que le noyau de l'action est réduite au sous-groupe $\{\mathrm{Id}, -\mathrm{Id}\}$. Il suffit pour cela de montrer que le noyau de ϕ est constitué d'homothéties, puisque les seules homothéties qui fixent par congruence une matrice non nulle sont Id et $-\mathrm{Id}$. Il suffit donc de montrer que toute droite est stabilisée par un élément du noyau, voir [H2G2, proposition II-4.3.6]. Par l'absurde, supposons qu'une matrice P de ${}^t(\ker\phi)$ (en assimilant matrice et morphisme via la base canonique de $\mathbb{C}^4$) envoie une droite D vers une droite D' distincte de D. Soit A une matrice antisymétrique telle que D

[8] *A posteriori*, ce résultat est vrai d'après l'exercice I-C.1.

soit dans le noyau de la forme bilinéaire associée à A (dans la même base canonique) et D' n'y soit pas. On peut bien entendu construire une telle matrice en partant de la matrice diagonale par blocs

$$B = \begin{pmatrix} 0 & 1 & & \\ -1 & 0 & & \\ & & 0 & 0 \\ & & 0 & 0 \end{pmatrix},$$

en effectuant une congruence par un changement de base qui envoie D sur $\mathbb{C}e_3$ et D' sur $\mathbb{C}e_1$. On a donc par construction l'égalité ${}^tPAP = A$, de sorte que l'image de D par P est dans le noyau A. Or, cette image est la droite D', qui a été choisie hors du noyau, d'où la contradiction.

La surjectivité résulte d'une méthode habituelle dans le contexte des groupes de Lie voir [H2G2, chapitre IX] : le morphisme ϕ étant différentiable (car polynomial), on a une différentielle $\mathrm{d}\phi : \mathfrak{sl}_4(\mathbb{C}) \to \mathfrak{so}_6(\mathbb{C})$. D'une part, $\mathrm{d}\phi$ est injective puisque le noyau de ϕ est discret. D'autre part, les résultats obtenus sur la description des algèbres de Lie permettent d'affirmer que $\dim \mathfrak{sl}_4(\mathbb{C}) = 4^2 - 1 = 15$ et $\dim \mathfrak{so}_6(\mathbb{C}) = 6 \times 5/2 = 15$. L'égalité de la dimension permet de voir que $\mathrm{d}\phi$ est un isomorphisme. Maintenant, le théorème d'inversion locale et la connexité de $\mathrm{SO}_6(\mathbb{C})$ permettent dans le cadre des morphismes de groupe de voir, comme dans la preuve de [H2G2, proposition X-2.1], que l'image de ϕ est bien $\mathrm{SO}_6(\mathbb{C})$ comme annoncé. □

Versant géométrique de $\mathrm{SL}_4(\mathbb{C})/\{\mathrm{Id}, -\mathrm{Id}\} \simeq \mathrm{SO}_6(\mathbb{C})$ sur un corps $\mathbb{K}$. Voici une petite digression géométrique. Le résultat que nous allons montrer se dit ainsi : il y a une bijection naturelle entre l'ensemble des droites de $\mathbb{P}^3$ et une quadrique de $\mathbb{P}^5$. Il peut être vu comme un corollaire de l'isomorphisme que nous venons de prouver, mais nous en donnons une preuve indépendante pour des raisons de simplicité, de canonicité et surtout, afin de travailler sur un corps $\mathbb{K}$ quelconque de caractéristique différente de 2.

Soit Q la quadrique projective d'équation $\mathrm{Pf}(A) = 0$ dans $\mathbb{P}(\mathscr{A}_4)$ (ce qui a un sens puisque Pf est homogène). On note que A dans Q est équivalent à dire que A est non nulle et de déterminant 0, c'est-à-dire de rang 2 (puisque le rang d'une matrice antisymétrique est pair). Soit $\mathrm{Gr}_{2,4}$ l'ensemble des plans dans $\mathbb{K}^4$. On définit les applications α et β suivantes :

$$\alpha : \mathrm{Gr}_{2,4} \to Q,\ F = \langle x, y\rangle \mapsto \mathbb{K}(x\,{}^ty - y\,{}^tx), \quad \beta : Q \to \mathrm{Gr}_{2,4},\ A \mapsto \mathrm{im}\, A.$$

2.14. Proposition. *Les applications α et β sont bien définies et réalisent des bijections réciproques entre la grassmannienne $\mathrm{Gr}_{2,4}$ et la quadrique projective Q. De plus, pour les actions naturelles, on a pour tout P de SL_4 la relation : $\alpha(P \cdot F) = P\alpha(F)\,{}^tP$.*

Démonstration. Montrons que α et β sont bien définies. En effet, si les vecteurs colonne x et y engendrent F, ils forment une base de F, si bien que la matrice $x\,{}^t y - y\,{}^t x$ est non nulle; de plus, il s'agit d'une matrice antisymétrique (puisque ${}^t(x\,{}^t y - y\,{}^t x) = -x\,{}^t y + y\,{}^t x$) et dont les colonnes sont des combinaisons linéaires de x et y. Cela implique que cette matrice est bien de rang 2, donc de déterminant nul. Si l'on choisit une autre base de F, alors un calcul rapide montre que l'on obtient une matrice (non nulle) proportionnelle à la première. Cela prouve notre assertion pour α. Pour β, c'est clair, car $\operatorname{im} A$ est bien de dimension 2 (une matrice antisymétrique est de rang pair et, ici, les rangs 0 et 4 sont exclus) et ne dépend pas de la matrice choisie sur la droite engendrée par A.

On a clairement $\beta\alpha = \mathrm{Id}$, par construction. Il suffit donc de montrer que α est surjective. Pour cela, supposons A antisymétrique de rang 2; alors, par définition, il existe deux vecteurs x et y indépendants tels que $A = x\,{}^t r + y\,{}^t s$, avec r et s vecteurs quelconques. L'égalité ${}^t A = -A$ implique : $r\,{}^t x + s\,{}^t y = -x\,{}^t r - y\,{}^t s$, puis : $\operatorname{im}(r\,{}^t x + s\,{}^t y) = \operatorname{im}(-x\,{}^t r - y\,{}^t s)$. Cela donne : $\langle r, s\rangle = \langle x, y\rangle$, de sorte que r et s sont dans le sous-espace $\langle x, y\rangle$. En écrivant r et s dans la base (x, y) et en utilisant le fait que $x\,{}^t x$, $x\,{}^t y$, $y\,{}^t x$, $y\,{}^t y$ sont des matrices indépendantes, on obtient, en caractéristique différente de 2 : $r = ky$ et $s = -kx$ pour k scalaire non nul. Comme A est non nulle, on obtient $A = k\big((x\,{}^t y - y\,{}^t x)\big)$, d'où le résultat.

La dernière assertion résulte des égalités :

$$\operatorname{im}\big(P(x\,{}^t y - y\,{}^t x)\,{}^t P\big) = \operatorname{im}\big((Px)\,{}^t(Py) - (Py)\,{}^t(Px)\big) = \langle Px, Py\rangle = P\langle x, y\rangle.$$

□

2.15. Remarque. Cette bijection entre grassmannienne et quadrique projective est parfois appelée *correspondance de Klein.* Mais, comme nous l'avons vu, le versant géométrique de l'isomorphisme $\mathrm{PSL}_2(\mathbb{C}) \simeq \mathrm{SO}_3(\mathbb{C})$ se voit comme un plongement de Veronese, et le versant géométrique de l'isomorphisme $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})/\{(\mathrm{I}_2, \mathrm{I}_2), (-\mathrm{I}_2, -\mathrm{I}_2)\} \simeq \mathrm{SO}_4(\mathbb{C})$ se voit comme un plongement de Segre, si bien que l'on voudrait terminer en beauté cette trilogie. Quel plongement généralise l'application α? N'atermoyons pas, le client est roi chez Calvage & Mounet : il s'agit du plongement de Plücker bien sûr, voir l'exemple I-2.6.

Revenons maintenant à l'isomorphisme exceptionnel. On ne peut pas échapper au corollaire classique du théorème 2.12. On rappelle pour cela que le groupe symplectique $\mathrm{Sp}_4(\mathbb{C})$ est inclus dans $\mathrm{SL}_4(\mathbb{C})$, voir le corollaire 1.21.

2.16. Corollaire. *L'isomorphisme* $\phi : \mathrm{SL}_4(\mathbb{C})/\{\mathrm{Id}, -\mathrm{Id}\} \simeq \mathrm{SO}_6(\mathbb{C})$ *fournit, par restriction, un isomorphisme* $\mathrm{Sp}_4(\mathbb{C})/\{\mathrm{Id}, -\mathrm{Id}\} \simeq \mathrm{SO}_5(\mathbb{C})$.

Démonstration. On note tout d'abord que $\{\mathrm{Id}, -\mathrm{Id}\} \subset \mathrm{Sp}_4(\mathbb{C})$. Soit alors P dans $\mathrm{Sp}_4(\mathbb{C})$; on a donc $PJ\,{}^tP = J$, où J est la matrice antisymétrique standard de $\mathscr{M}_4(\mathbb{C})$, voir 1.1. Soit $\bar{P}$ sa classe dans $\mathrm{Sp}_4(\mathbb{C})/\{\mathrm{Id}, -\mathrm{Id}\} \subset \mathrm{SL}_4(\mathbb{C})/\{\mathrm{Id}, -\mathrm{Id}\}$, on peut dire que $\phi(\bar{P})$ est un élément du groupe orthogonal $\mathrm{SO}_6(\mathbb{C})$ qui fixe J, et donc qui stabilise son orthogonal dans $\mathscr{A}_4(\mathbb{C})$, lequel est de dimension 5. Comme J ne dépend pas de P, on peut voir $\phi(\bar{P})$ dans le sous-groupe de $\mathrm{SO}_6(\mathbb{C})$ laissant fixe le sous-espace $J^\perp$ et l'on obtient un morphisme injectif (car ϕ l'est) de $\mathrm{Sp}_4(\mathbb{C})/\{\mathrm{Id}, -\mathrm{Id}\}$ vers $\mathrm{SO}_5(\mathbb{C})$.

Comme dans la preuve du théorème précédent, et comme $\mathrm{SO}_5(\mathbb{C})$ est connexe, il reste à montrer que les algèbres de Lie $\mathfrak{sp}_4(\mathbb{C})$ et $\mathfrak{so}_5(\mathbb{C})$ sont de même dimension. On a : $\dim \mathfrak{so}_5(\mathbb{C}) = 5 \times 4/2 = 10$. On a de plus : $\mathfrak{sp}_4(\mathbb{C}) = \{M,\ MJ + J\,{}^tM = 0\}$. Cette équation se résout en écrivant M par blocs 2×2 : de la relation

$$\begin{pmatrix} A & C \\ B & D \end{pmatrix}\begin{pmatrix} 0 & \mathrm{I}_2 \\ -\mathrm{I}_2 & 0 \end{pmatrix} = -\begin{pmatrix} 0 & \mathrm{I}_2 \\ -\mathrm{I}_2 & 0 \end{pmatrix}\begin{pmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{pmatrix},$$

on tire aisément que ${}^tA = -C$ et que B, C sont symétriques. Il vient : $\dim \mathfrak{sp}_4(\mathbb{C}) = 4 + 3 + 3 = 10 = \dim \mathfrak{so}_5(\mathbb{C})$, coïncidence numérique qui donne le résultat voulu. □

3. Grassmanniennes de signature donnée et application aux faisceaux de cercles

On va classer ici les *faisceaux de cercles* du plan (ou plutôt de la droite complexe $\mathbb{P}^1(\mathbb{C})$) et observer les *dégénérescences de faisceaux* modulo l'action de $\mathbb{P}^1(\mathbb{C})$. Selon la stratégie de [H2G2, §XI-3.5], qui sera brièvement réexpliquée, cela revient à classer les plans de $\mathbb{R}^4$ modulo l'action $\mathrm{SO}_0(3,1)$.

Il n'est en fait pas plus difficile de regarder ce dernier problème dans le cadre général de l'action de $\mathrm{SO}_0(s,t)$ sur une grassmannienne de $\mathbb{R}^n$, où $n = s+t$. Cette action nous définit des orbites : l'ensemble des « grassmanniennes de signature et de dimension données ». Par la suite, comme nous en avons désormais l'habitude, nous pourrons définir ces grassmanniennes comme des espaces homogènes et en déduire des propriétés topologiques.

Encore une fois, le plaisir est dans l'unité de la démarche, ramenant un problème de faisceaux de cercles à une action naturelle de groupes classiques sur des grassmanniennes.

On supposera toujours dans la suite $st \neq 0$. Le cas $st = 0$ se ramène à la situation des espaces euclidiens, où la situation est bien plus simple.

LLU PRODUIT DE L'ANNÉE

3.1. Proposition. *Soit q une forme quadratique non dégénérée de signature (s,t) sur $\mathbb{R}^n$, et soit F un sous-espace de $\mathbb{R}^n$ de dimension m. La signature (s',t') de la restriction de q à F est telle que*

$$s' \leqslant s,\ t' \leqslant t,\ s'+t' \leqslant m \leqslant \min(s+t', s'+t).$$

Réciproquement, si s' et t' sont deux entiers positifs qui vérifient ces inégalités, alors il existe un sous-espace F de dimension m tel que la restriction de q à F soit de signature (s',t').

Démonstration. Rappelons de [H2G2, §V-1] que r (resp. s) est la dimension maximale d'un sous-espace sur lequel la restriction de q est définie positive (resp. définie négative). Les inégalités $s' \leqslant s$ et $t' \leqslant t$ en résultent. Comme $s'+t'$ est le rang de la restriction de q à F, on a l'inégalité $s'+t' \leqslant \dim(F) = m$. De plus, de par la classification des formes quadratiques réelles, on sait que tout F se décompose en une somme directe $F_{\geqslant 0} \oplus F_{<0}$ telle que la restriction de q à $F_{\geqslant 0}$ (resp. $F_{<0}$) soit positive (resp. définie négative). Par construction, on a : $\dim F_{<0} = t'$. De plus, $F_{\geqslant 0}$ ne peut pas intersecter non trivialement un sous-espace sur lequel q est définie négative, et donc par la formule de Grassmann, on a nécessairement $\dim F_{\geqslant 0} \leqslant n - t = s$. Conclusion : $m = \dim F = \dim F_{\geqslant 0} + \dim F_{<0} \leqslant s + t'$. La dernière inégalité est analogue.

Réciproquement, on suppose ces inégalités vérifiées et l'on veut trouver un sous-espace F de dimension m tel que $q|_F$ soit de signature (s',t'). Pour cela, on dispose d'une base $(e_1, \ldots, e_s, e_{s+1}, \ldots, e_n)$ de $\mathbb{R}^n$ telle que la matrice de q dans cette base soit de forme normale $\mathrm{I}_{s,t}$. Posons $k = m - s' - t'$. Les inégalités impliquent $0 \leqslant k \leqslant \min(s-s', t-t')$ et donc $s+k+t' \leqslant n$, puisque $t = n - s$. On vérifie alors que le sous-espace F engendré par

$$(e_1 + e_{s+1}, \ldots, e_k + e_{s+k}, e_{k+1}, \ldots, e_{k+s'}, e_{s+k+1}, \ldots, e_{s+k+t'})$$

satisfait bien à la propriété voulue : les éléments e_i dans le système ci-dessus existent bel et bien puisque $s+k+t' \leqslant n$, les vecteurs sont tous orthogonaux, il y en a exactement m, les k premiers sont isotropes, les s' suivants sont positifs (car $k+s' \leqslant s$) et les t' derniers sont négatifs. □

On dit alors dans ce contexte que F est de dimension m et de signature (s',t') *admissibles*. Il est maintenant naturel de chercher un résultat de classification des orbites de la grassmannienne pour l'action de $\mathrm{SO}_0(s,t)$.

3.2. Exemple. Soit q une forme quadratique de signature $(3,1)$ sur $\mathbb{R}^4$. Alors, la signature de la restriction de q sur un plan de $\mathbb{R}^4$ ne peut être que $(2,0)$, $(1,1)$ ou $(1,0)$.

3.3. Proposition. *Soit l'espace $\mathbb{R}^n$ muni d'une forme non dégénérée de signature (s,t). On suppose $s \neq t$. Alors, les orbites de l'action de $\mathrm{SO}_0(s,t)$ sur la grassmannienne de $\mathbb{R}^n$ sont classées par la dimension et la signature (admissibles). Une grassmannienne de signature et dimension données est connexe et compacte pour la topologie induite sur elle-même.*

Démonstration. Soit F un sous-espace de dimension m, de signature (s',t') et soit g dans $\mathrm{O}(s,t)$. Alors, g est une isométrie de F vers $g(F)$, et donc $g(F)$ a même signature que F (et même dimension !). Inversement, si F et F' ont même dimension et même signature, alors il existe une isométrie de F vers F', et, par le théorème de Witt [H2G2, V-3.4], cette isométrie fournit un élément g de $\mathrm{O}(s,t)$ qui envoie F sur F'.

Il reste à montrer que l'on peut trouver g dans $\mathrm{SO}_0(s,t)$. Rappelons que comme m et (s',t') satisfont aux inégalités voulues, on peut se ramener, par transitivité de l'action de $\mathrm{O}(s,t)$ sur la grassmannienne de signature (s',t'), au cas où le sous-espace F est le sous-espace F_0 engendré par

$$(e_1 + e_{s+1}, \dots, e_k + e_{s+k}, e_{k+1}, \dots, e_{k+s'}, e_{s+k+1}, \dots, e_{s+k+t'}),$$

avec $k = m - s' - t'$.

L'hypothèse $s \neq t$ implique facilement qu'il existe r tel que $r \notin \{1, \dots, k, s+1, \dots, s+k\}$. On peut définir g_F qui envoie e_r sur $-e_r$ et e_i sur e_i pour $i \neq r$. Ainsi, g_F est une isométrie de déterminant -1 dans le stabilisateur de F. Soit $\mathscr{O}_F$ l'orbite de F pour l'action de $\mathrm{O}(s,t)$, c'est-à-dire la grassmannienne des sous-espaces de dimension m et de signature (s',t'). Comme $\mathrm{SO}(s,t)$ est d'indice 2 dans $\mathrm{O}(s,t)$, on a

$$\mathscr{O}_F = \mathrm{O}(s,t) \cdot F = \mathrm{SO}(s,t) \cdot F \cup \big(\mathrm{SO}(s,t) g_F\big) \cdot F = \mathrm{SO}(s,t) \cdot F.$$

Cela prouve que l'action de $\mathrm{SO}(s,t)$ reste transitive sur $\mathscr{O}_F$. On voit de même que l'isométrie g'_F qui envoie e_1 sur $-e_1$, e_{s+1} sur $-e_{s+1}$ et e_i sur e_i pour i distinct de 1 et $s+1$, appartient au stabilisateur de F et à $\mathrm{SO}(s,t)$, mais n'appartient pas à $\mathrm{SO}_0(s,t)$, voir la construction de $\mathrm{SO}_0(s,t)$ dans [H2G2, corollaire VII-A.5]. De manière analogue, on obtient donc

$$\mathscr{O}_F = \mathrm{SO}(s,t) \cdot F = \mathrm{SO}_0(s,t) \cdot F \cup \big(\mathrm{SO}_0(s,t) g'_F\big) \cdot F = \mathrm{SO}_0(s,t) \cdot F.$$

Cela prouve la transitivité ainsi que la connexité de $\mathscr{O}_F$, puisque l'action du groupe connexe $\mathrm{SO}_0(s,t)$ est continue.

Montrons que l'orbite $\mathscr{O}_F$ est compacte. Soit π la projection de $\mathrm{GL}_n(\mathbb{R})$ sur le quotient $\mathrm{GL}_n(\mathbb{R})/P$ par le stabilisateur d'un sous-espace F donné, pour l'action naturelle de $\mathrm{GL}_n(\mathbb{R})$. L'application π est ouverte et surjective, donc elle envoie le fermé $\mathrm{O}(s,t)$ de $\mathrm{GL}_n(\mathbb{R})$ sur le fermé $\mathrm{O}(s,t)/P \cap \mathrm{O}(s,t)$ de $\mathrm{GL}_n(\mathbb{R})/P$. Par le théorème d'homéomorphisme, $\mathrm{O}(s,t)/P \cap \mathrm{O}(s,t)$ est homéomorphe à l'orbite $\mathrm{O}(s,t) \cdot F$ qui est donc fermé dans la grassmannienne $\mathrm{GL}_n(\mathbb{R}) \cdot F$. Comme la grassmannienne est compacte, il en découle la compacité de l'orbite $\mathrm{O}(s,t) \cdot F$. □

3.4. Remarque. Attention, ces grassmanniennes à signature donnée ne sont pas fermées pour la topologie induite sur la grassmannienne. Un sous-espace de signature donnée peut dégénérer en un sous-espace de signature différente (mais inférieure). On verra un exemple d'une telle situation au moment de l'étude des faisceaux de cercles.

3.5. Remarque. Si $s = t$, et donc $n = 2s$, la proposition reste essentiellement valable avec une preuve analogue, sauf pour le cas de la grassmannienne de signature $(0,0)$ et de dimension $s = n/2$. Cette grassmannienne est alors l'ensemble des SETIM et celle-ci possède deux composantes connexes et deux orbites pour $\mathrm{SO}_0(s,s)$. Voir [H2G2, exercice V-D.22].

3.6. Étude des faisceaux de cercles de $\mathbb{P}^1(\mathbb{C})$

Au moment de la preuve de l'alternative de Steiner ([H2G2, §XI-3]), nous avons réalisé l'ensemble $\mathscr{D}\mathscr{C}$ des cercles de $\mathbb{P}^1(\mathbb{C})$ (ou « cercles ou droites » du plan[9]) comme une partie de l'espace projectif $\mathbb{P}^3(\mathbb{R})$ « muni » d'une forme quadratique de signature $(3,1)$. Faisons quelques rappels du tome premier.

On sait associer, à un élément de $\mathscr{D}\mathscr{C}$, son équation réduite, de la forme $ax^2 + ay^2 + 2bx + 2cy + d = 0$, l'élément $(a : b : c : d)$ de $\mathbb{P}^3(\mathbb{R})$. L'ensemble des équations $u \in \mathbb{R}^4$ correspondant à un cercle non vide et non réduit à un point est donné par la contrainte $q(u) > 0$, où $q(a,b,c,d) = b^2 + c^2 - ad$. On voit que q est une forme quadratique de signature $(3,1)$. Soit donc $\mathbb{R}^4_{q>0} = \{u \in \mathbb{R}^4,\ q(u) > 0\}$ l'extérieur du cône isotrope de q. On définit une correspondance

$$\alpha : \mathbb{R}^4_{q>0} \to \mathscr{D}\mathscr{C}$$

qui envoie (a,b,c,d) sur le cercle d'équation $ax^2 + ay^2 + 2bx + 2cy + d = 0$, et établissant une bijection $\bar{\alpha} : \mathbb{R}^4_{q>0}/\mathbb{R}^* \simeq \mathscr{D}\mathscr{C}$.

Faisons maintenant agir les groupes. D'un côté, le groupe $\mathrm{SO}_0(q)$, qui est isomorphe à $\mathrm{SO}_0(3,1)$, agit sur $\mathbb{R}^4$ en laissant stable $\mathbb{R}^4_{q>0}$. D'un autre côté, le groupe $\mathrm{PSL}_2(\mathbb{C})$ agit de façon naturelle sur $\mathbb{P}^1(\mathbb{C})$ et donc sur $\mathscr{D}\mathscr{C}$. Résumons [H2G2, proposition XI-3.5.4] et [H2G2, proposition IX-2.3].

3.7. Proposition. *Il existe un isomorphisme*[10] $\iota : \mathrm{SO}_0(q) \to \mathrm{PSL}_2(\mathbb{C})$ *tel que* $\bar{\alpha}$ *entrelace l'action du groupe orthogonal sur les formes et l'action des homographies sur les cercles : pour* $g \in \mathrm{SO}_0(q)$ *et* $u \in \mathbb{R}^4_{q>0}$, *on a :* $\bar{\alpha}\big(g(u)\big) = \iota(g)\big(\bar{\alpha}(u)\big)$.

[9] Nous nous dispenserons dans la suite de le préciser.

[10] Exceptionnel, comme il se doit...

Ainsi, l'isomorphisme exceptionnel entre $\mathrm{PSL}_2(\mathbb{C})$ et $\mathrm{SO}_0(q)$ permet de ramener l'étude de la classification des cercles de $\mathbb{P}^1(\mathbb{C})$ modulo l'action de $\mathrm{PSL}_2(\mathbb{C})$ à la classification correspondante dans $\mathbb{R}^4$ modulo l'action de $\mathrm{SO}_0(q)$. Un cercle correspondant à une droite de $\mathbb{R}^4$ sur laquelle q est positive. Or, celle-ci se fait sans trop d'encombre grâce au théorème de Witt, plus précisément, la transitivité de l'action du sous-groupe $\mathrm{SO}_0(q)$ d'indice 4 sur les droites de signature $(1,0)$, voir la proposition 3.3.

Il serait dommage, à ce stade, de passer à côté de la classification des faisceaux de cercles qui peut se faire agréablement à l'aide de cette même correspondance.

En effet, un faisceau de cercles est un ensemble de cercles dont l'équation est une combinaison linéaire de deux équations indépendantes de cercles données, c'est-à-dire, via la correspondance, un sous-espace de $\mathbb{R}^4$ de dimension 2 (auquel on enlève le vecteur nul). Bien entendu, il faut comprendre qu'il s'agit en réalité de l'intersection de ce plan ainsi défini avec l'extérieur du cône isotrope de q, l'intérieur ne correspondant pas à de vrais cercles.

3.8. Définition. On appelle *faisceau de cercles* une partie de $\mathscr{DC}$ définie par $\alpha(xu + x'u')$, où u et u' sont fixés dans $\mathbb{R}^4_{q>0}$, et où (x, x') parcourt l'ensemble des couples de réels tels que $xu + x'u'$ soit dans $\mathbb{R}^4_{q>0}$.

Autrement dit, c'est une partie de $\mathscr{DC}$ constituée de tous les cercles de $\mathbb{P}^1(\mathbb{C})$ dont les équations sont combinaisons linéaires de celles de deux cercles donnés.

On voit arriver deux questions naturelles, dans l'ordre.

3.9. Question. Peut-on reconnaître un plan à partir de son intersection avec l'extérieur $\mathbb{R}^4_{q>0}$ du cône ?

3.10. Question. Comment classer les plans de $\mathbb{R}^4$ modulo l'action $\mathrm{SO}_0(q)$?

Pour ce qui est de la question 3.9, la réponse est positive. En effet, d'après l'exemple 3.2, l'intersection du plan avec l'extérieur $\mathbb{R}^4_{q>0}$ du cône est un ouvert du plan. Et donc, le plan peut être reconstitué à partir de cet ouvert.

Pour la question suivante, on va commencer par fixer deux points distincts A et A' dans $\mathbb{C}$ et donner trois exemples de faisceaux de cercles.

1. *L'ensemble des éléments de $\mathscr{DC}$ passant par A et A'.*
   En effet, on voit que l'ensemble des $(a, b, c, d) \in \mathbb{R}^4$ tels que l'équation $ax^2 + ay^2 + 2bx + 2cy + d = 0$ est vérifiée pour deux points distincts (x_A, y_A), $(x_{A'}, y_{A'})$ est une intersection de deux hyperplans distincts. C'est donc bien un plan P de $\mathscr{H}^2(\mathbb{C})$. De plus, comme chacune de ces équations dmet au moins deux solutions, elles définissent bien un élément de $\mathscr{DC}$, si bien que l'intersection de P et de $\mathbb{R}^4_{q>0}$ est $P \setminus \{0\}$.

2. *L'ensemble des éléments $C_{(x,x')}$ de $\mathscr{DC}$ définis, pour $(x,x') \in \mathbb{R}^2$, par $C_{(x,x')} = \{M,\ xAM^2 - x'A'M^2 = 0\}$.*

   D'une part, on voit que les équations définissent bien un plan de $\mathbb{R}^4$. D'autre part, une condition nécessaire et suffisante pour que l'équation $xAM^2 - x'A'M^2 = 0$ définisse un cercle ou une droite est que $xx' > 0$. En effet, si $xx' \leqslant 0$ l'ensemble est vide ou réduit à un point. Si $xx' > 0$, alors l'équation définit le lieu des points M tels que le rapport $AM/A'M$ est une constante positive fixée. Il s'agit bien d'un élément de $\mathscr{DC}$. Cette fois-ci, le plan n'est pas entièrement inclus dans $\mathbb{R}^4_{q>0}$. L'intersection de P et de $\mathbb{R}^4_{q>0}$ est l'intérieur d'un cône (quadratique, car c'est l'intersection d'un plan et de l'intérieur d'une quadrique).

3. *La partie formée des cercles passant par A et dont la tangente en A est la droite $D = AA'$, partie à laquelle on ajoute naturellement la droite (AA').*

   En effet, quitte à faire deux cas selon que a vaut 0 ou non, on voit que ces conditions impliquent le système d'équations $ax_A^2 + ay_A^2 + 2bx_A + 2cy_A + d = 0$, $(x_{A'} - x_A)(ax_A + b) + (y_{A'} - y_A)(ay_A + c) = 0$ et l'on vérifie que ces conditions sur (a,b,c,d) définissent un plan P de $\mathbb{R}^4$. Réciproquement, ce système fournit des solutions (a,b,c,d) qui correspondent à une droite ou un cercle, sauf dans le cas où (x_A, y_A) est le seul point vérifiant $ax^2 + ay^2 + 2bx + 2cy + d = 0$, c'est-à-dire, en utilisant la décomposition canonique du trinôme, si et seulement si $(b,c) = (-ax_A, -ay_A)$. L'intersection de P et de $\mathbb{R}^4_{q>0}$ est le plan P auquel on a ôté une droite.

Dans le cas 1, on dit que l'on a un faisceau à points bases A et A'. Dans le cas 2, un faisceau à points limites A et A'. Dans le cas 3, on dit que l'on a un faisceau de cercles tangents en A. Voir figures ci-après[11].

La question 3.10 vient d'être étudiée dans les propositions 3.1 et 3.3, dans le cadre plus général de l'action de $\mathrm{SO}_0(s,t)$ sur une grassmannienne de $\mathbb{R}^n$, où $n = s+t$. Il suffit donc de trouver dans ce cas précis les plans admissibles.

Nous allons voir que les seuls cas possibles sont ceux cités ci-dessus, mais puisque que nous travaillons dans le contexte de la géométrie projective, nous devons ajouter le cas où le point A est à l'infini. Le faisceau de droites passant par A' sera donc un faisceau à points bases ∞ et A'. Le faisceau de cercles centré en A' sera un faisceau à points limites ∞ et A'. Et, le faisceau de droites parallèles de direction donnée D sera un faisceau de cercles tangents en l'infini.

[11] Mise en garde : ces images peuvent provoquer des désordres dans les zones visuelles du cerveau.

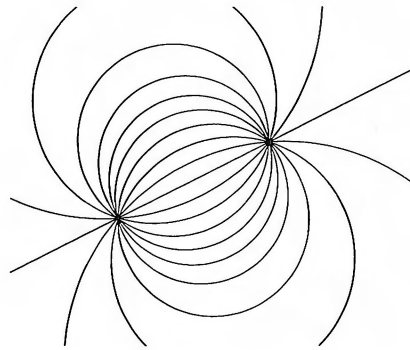


Figure 3.1. *Faisceau à points bases*

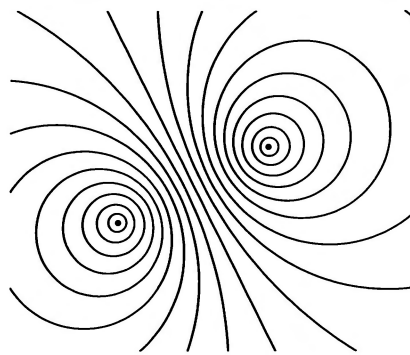


Figure 3.2. *Faisceau à points limites*

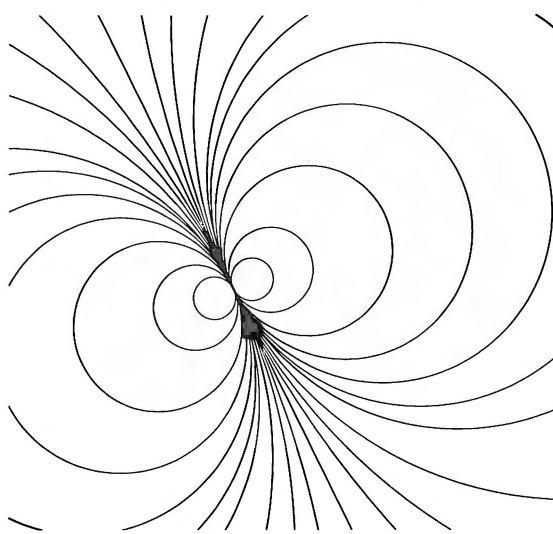


Figure 3.3. *Faisceau tangent*

3.11. Proposition. *Il y a exactement trois types de faisceaux de cercles dans $\mathscr{D}\mathscr{C}$: les faisceaux à points bases, les faisceaux à points limites et les faisceaux de cercles tangents. Autrement dit, l'action naturelle de* $\mathrm{PSL}_2(\mathbb{C})$ *sur l'ensemble des faisceaux de cercles possède trois orbites associées aux trois types de faisceaux présentés ci-dessus, et ces trois orbites correspondent via α aux orbites sous* $\mathrm{SO}_0(q)$ *des plans de signatures respectives* $(2,0)$, $(1,1)$, $(1,0)$.

Démonstration. Dans l'espace $\mathbb{R}^4$ muni de la forme quadratique $q = -\det$, de signature $(3,1)$, on considère donc la grassmannienne des plans. Par l'exemple 3.2, la restriction $\bar{q}_P$ de q à un plan P fixé est de signature $(2,0)$, $(1,1)$ ou $(1,0)$.

La signature de $\bar{q}_P$ peut prendre trois valeurs : $(2,0)$ $(1,1)$ et $(1,0)$; le discriminant de $\bar{q}_P$ vaut alors respectivement 1, -1 et 0. Or, si l'on choisit une base (H,H') de P correspondant à deux cercles C_H et $C_{H'}$, le discriminant de $\bar{q}_P$ est égal au signe de $\varphi(H,H')^2 - q(H)q(H')$ (c'est-à-dire au signe de l'*invariant anallagmatique* de C_H et $C_{H'}$), qui, selon les trois cas, appartient respectivement à $]-1,1[$, $]-\infty,-1[\cup]1,+\infty[$, $\{-1,1\}$. On sait alors, par [H2G2, corollaire XI-3.5.7], que dans le premier cas, C_H et $C_{H'}$ s'intersectent en deux points; dans le deuxième, il ne s'intersectent pas et dans le troisième, ils sont tangents. Le faisceau $\alpha(P)$ est donc d'un des trois types cités. Par la proposition 3.7 et la proposition 3.3, $\mathrm{PSL}_2(\mathbb{C})$ agit donc sur chacun des trois types de faisceaux, et cette action est transitive. □

3.12. Faisceaux orthogonaux

On rappelle que si H et H' sont q-orthogonaux dans $\mathbb{R}^4_{q>0}$, les cercles C_H et $C_{H'}$ correspondants ont alors un invariant anallagmatique nul ([H2G2, corollaire XI-3.5.7]), et se coupent donc orthogonalement (au sens de l'orthogonalité courante de l'espace hermitien $\mathbb{C}$) en deux points de $\mathbb{P}^1(\mathbb{C})$ (si ce sont deux droites, elles sont concourantes en deux points, dont l'infini !). Si F est un faisceau de cercles, alors l'ensemble $F^\perp$ des cercles orthogonaux à tous les cercles de F est encore un faisceau de cercles puisqu'il correspond, via α, au plan orthogonal $P_F^\perp$, où P_F est le plan de $\mathbb{R}^4$ correspondant à F.

Or, si P_F est un plan de signature $(2,0)$, il est non dégénéré, donc son orthogonal pour q lui est supplémentaire. Puisque la forme q est de signature $(3,1)$, on obtient que son orthogonal $P_F^\perp$ est un plan de signature $(1,1)$. Inversement, si P_F est de signature $(1,1)$, son orthogonal sera de signature $(2,0)$. Maintenant, si P_F est un plan de signature $(1,0)$, alors par élimination dans la proposition 3.11, son orthogonal est un plan de signature $(1,0)$.

3.13. Corollaire. *Le groupe* $\mathrm{PSL}_2(\mathbb{C})$ *agit sur les paires de faisceaux de cercles orthogonaux. Il y a deux orbites pour cette action : une orbite de paires constituées d'un faisceau à points bases et du faisceau orthogonal à points limites, et une orbite de paires constituées de deux faisceaux de cercles tangents orthogonaux.*

Démonstration. On vient de classifier les paires de faisceaux orthogonaux en fonction de la signature. Le corollaire se montre en appliquant la proposition 3.3 et en remarquant que si $g \in \mathrm{SO}_0(q)$ envoie le plan P sur le plan P', alors, il envoie $P^\perp$ sur $P'^\perp$. □

On illustre ces deux situations par les figures 3.4 et 3.5 de faisceaux génériques.

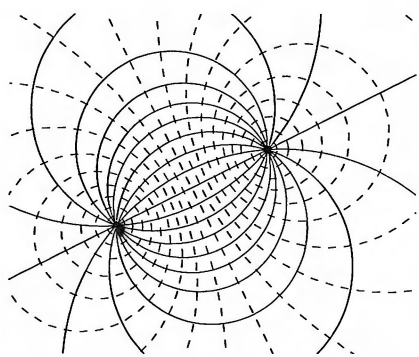


Figure 3.4. *Faisceau à points bases et son orthogonal à points limites*

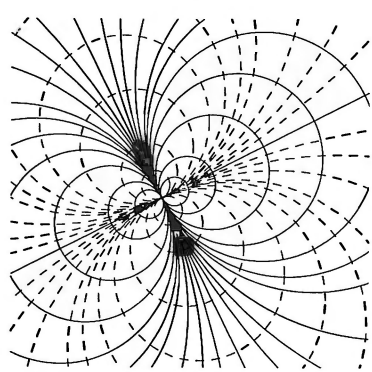


Figure 3.5. *Faisceau de cercles tangent et son orthogonal de cercles tangent*

On peut préférer les « formes normales » des figures 3.6 et 3.7 pour chaque situation.

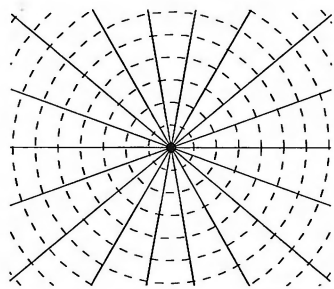


Figure 3.6. *Faisceau à points bases* 0 *et* ∞ *et son orthogonal à points limites*

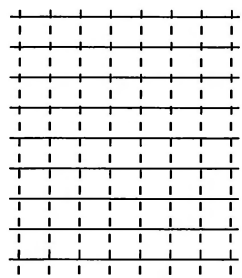


Figure 3.7. *Faisceau tangent « basé en l'infini » et son orthogonal*

3.14. Étude topologique des faisceaux de cercles

Si nous voulons rester honnêtes dans notre démarche, il nous faut encore donner un dernier coup de collier en faisant une étude topologique de ces faisceaux. Via α, on peut les transporter dans la grassmannienne des plans de $\mathbb{R}^4$, et l'ensemble des faisceaux peut donc être muni d'une topologie par transport de structure. Comme d'habitude, la continuité de l'action de $\mathrm{GL}(\mathbb{R}^4)$ sur la grassmannienne assure la continuité de $\mathrm{SO}_0(q)$ sur cette même grassmannienne et, par transport de structures, que l'adhérence d'une orbite de faisceaux pour l'action de $\mathrm{PSL}_2(\mathbb{C})$ est encore une orbite de faisceaux.

3.15. Proposition. *Soit* $\mathscr{F}$ *l'ensemble des faisceaux muni de la topologie de la grassmannienne des plans de* $\mathbb{R}^4$ *par transport de structure. Alors, les ensembles respectifs* $\mathscr{F}_b$, $\mathscr{F}_\ell$ *et* $\mathscr{F}_t$ *des faisceaux à points bases, des faisceaux à points limites et des faisceaux de cercles tangents sont connexes. On a de plus les adhérences suivantes :*

$$\overline{\mathscr{F}_b} = \mathscr{F}_b \cup \mathscr{F}_t,\ \overline{\mathscr{F}_\ell} = \mathscr{F}_\ell \cup \mathscr{F}_t,\ \overline{\mathscr{F}_t} = \mathscr{F}_t.$$

Ces adhérences sont compactes pour la topologie de $\mathscr{F}$.

Démonstration. Les propriétés de connexité et de compacité proviennent de la proposition 3.3. Reste à montrer les assertions sur les dégénérescences. Tout d'abord, on sait d'après ce qui précède que l'adhérence d'une orbite est encore une orbite. Donc, pour la première égalité, il suffit de montrer qu'une suite de $\mathscr{F}_b$ ne peut converger vers un élément de $\mathscr{F}_\ell$ et qu'il existe une suite de $\mathscr{F}_b$ qui converge vers un faisceau de cercles tangents. On va montrer cela dans le cadre des grassmanniennes de plans.

Soit donc une suite de plans $(P_n)_{n\in\mathbb{N}}$ de signature $(2,0)$ qui converge vers un plan P. On doit montrer que le plan P n'est pas de signature $(1,1)$. On rappelle que le théorème d'homéomorphisme dit que la grassmannienne de signature $(2,0)$, étant une orbite sous l'action de $\mathrm{SO}_0(q)$, est homéomorphe à un quotient de ce groupe. Soit $X = \{P_n,\ n \in \mathbb{N}\}$; on a donc : $\overline{X} = \{P_n,\ n \in \mathbb{N}\} \cup \{P\}$. Comme la projection canonique $\pi : \mathrm{SO}_0(q) \to \mathrm{SO}_0(q)/\mathrm{SO}_0(q)_{P_1}$ est surjective, continue et fermée, on voit par une double inclusion que $\pi^{-1}(\overline{X}) = \overline{\pi^{-1}(X)}$. Résultat : une suite de $\pi^{-1}(X)$ qui converge, converge dans $\pi^{-1}(\overline{X})$ et tout élément de $\pi^{-1}(\overline{X})$ peut être atteint par une suite de $\pi^{-1}(X)$. On peut donc relever la suite (P_n) (à partir d'un certain rang) en une suite (g_n) de $\mathrm{SO}_0(q)$ qui converge vers un élément g de $\mathrm{SO}_0(q)$ et telle que $g_n \cdot P_1 = P_n$ converge vers $g \cdot P_1 = P$.

Maintenant, si v est un vecteur de P, il peut s'écrire $v = g \cdot v_1$ avec v_1 dans P_1 et donc, v est limite de la suite $g_n(v_1)$. Comme la forme quadratique q est continue, que $q\big(g_n(v_1)\big)$ est positif (ou nul) par définition et que $\mathbb{R}^+$ est fermé, il vient que $q(v)$ est également positif ou nul. Comme on a choisi v quelconque dans P, la signature de P ne peut être $(1,1)$.

Montrons maintenant qu'il existe une suite de $\mathscr{F}_b$ qui converge vers un faisceau de $\mathscr{F}_t$. Par le théorème de Sylvester, on peut trouver une base $\mathbf{e} = (e_1, e_2, e_3, e_4)$ de $\mathbb{R}^4$ telle que la matrice de q dans cette base soit

$$\mathrm{mat}(q) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Soit P le plan engendré par (e_1, e_3). Il est de signature $(1,0)$. Pour n entier naturel non nul, soit g_n l'automorphisme de P dont la matrice dans $\mathbf{e}$ est

$$\mathrm{mat}(g_n) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \frac{1}{n} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Alors, la suite $\big(g_n(P)\big)_{n\geqslant 1}$ est une suite de plans de signature $(2,0)$ qui converge vers le plan P de signature $(1,0)$.

Les autres preuves sont complètement analogues et laissées à la perspicacité du lecteur. □

3.16. Remarque. Il est très intuitif qu'une suite de faisceaux à points bases (ou à points limites) puisse converger vers un faisceau de cercles tangents. On imagine visuellement la paire de points bases (ou limites) converger vers un seul point A dans une direction donnée D et définir ainsi par passage à la limite un faisceau de cercles tangents en A, avec $D^\perp$ comme tangente en A. Mais, la mise en place d'une telle approche demande l'intervention d'une topologie sur les paires de points, et l'on voit l'utilité des schémas de Hilbert, voir [H2G2, exercice II-F.34].

3.17. Remarque. On a sciemment présenté une preuve abstraite pour montrer que ce phénomène de dégénérescence est plus général. L'adhérence d'une grassmannienne (supposée non vide) de signature (s,t) contient une grassmannienne (non vide) de signature (s',t') si et seulement si $s' \leqslant s$ et $t' \leqslant t$. On laisse cette preuve au lecteur, en donnant l'indication suivante au lecteur : dans la démonstration précédente, remplacer le vecteur v dans P par un sous-espace maximal positif (ou négatif) pour la forme quadratique.

3.18. Faisceaux et sous-groupes à un paramètre

Dans ce bref paragraphe, on réinterprète les faisceaux de cercles comme des familles d'orbites pour les sous-groupes à un paramètre « réels » de $\mathrm{SL}_2(\mathbb{C})$. Rappelons qu'un sous-groupe à un paramètre de $\mathrm{SL}_2(\mathbb{C})$ est un morphisme continu de $\mathbb{R}$ dans $\mathrm{SL}_2(\mathbb{C})$. D'après [H2G2, proposition IX-A.6.1], ils sont tous de la forme $\varphi_X : t \mapsto \exp(tX)$ pour X dans l'espace $\mathfrak{sl}_2(\mathbb{C})$ des matrices 2×2 de trace nulle. On dit que le sous-groupe à un paramètre est *réel* si X appartient à $\mathfrak{sl}_2(\mathbb{R})$.

Fixons X dans $\mathfrak{sl}_2(\mathbb{R})$ non nulle. Comme on s'intéresse aux orbites de l'image T de φ_X, on peut multiplier X par une constante non nulle c, ce qui revient à précomposer φ_X par $t \mapsto c^{-1}t$. Autrement dit, la vraie donnée de départ est un point du plan projectif $\mathbb{P}\big(\mathfrak{sl}_2(\mathbb{R})\big)$. Trois cas sont possibles.

Type elliptique. On parle de sous-groupe *de type elliptique* lorsque X possède deux valeurs propres complexes non réelles. Comme sa trace est nulle, elles sont nécessairement imaginaires pures, disons ia et $-ia$ avec $a \in \mathbb{R}^{+*}$. Quitte à remplacer X par $a^{-1}X$, on peut supposer que $a = 1$, de sorte que X est semblable à

$$X_- = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

L'image de φ_{X_-} dans $\mathrm{PSL}_2(\mathbb{R})$ est formée des homographies $z \mapsto e^{2it}z$ ($t \in \mathbb{R}$). Ses orbites dans $\mathbb{P}^1(\mathbb{C})$ sont ∞, 0 et les cercles centrés en 0.

Conjuguer X_- par un élément quelconque de $\mathrm{GL}_2(\mathbb{C})$ a pour effet de conjuguer le sous-groupe à un paramètre par une homographie h quelconque. Les

orbites de ce sous-groupe sont les images des orbites, c'est-à-dire les deux points $h(\infty)$ et $h(0)$ et les arcs des cercles du faisceau à points limites qu'ils définissent.

Type parabolique. On parle de sous-groupe *de type parabolique* lorsque X possède pour seule valeur propre 0. La matrice X est nilpotente non nulle donc semblable à

$$X_0 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

L'image de φ_{X_0} dans $\mathrm{PSL}_2(\mathbb{R})$ est formée des homographies $z \mapsto z + t$ ($t \in \mathbb{R}$). Ses orbites dans $\mathbb{P}^1(\mathbb{C})$ sont ∞ et les droites de $\mathbb{C}$ parallèles à l'axe réel. Autrement dit, ce sont le point ∞ et les cercles d'un faisceau tangent en ce point (figure 3.7).

Conjuguer X_0 par un élément quelconque de $\mathrm{GL}_2(\mathbb{C})$ a pour effet de conjuguer le sous-groupe à un paramètre par une homographie h quelconque. Les orbites de ce sous-groupe sont les images des orbites, c'est-à-dire le point $h(\infty)$ et les cercles d'un faisceau tangent qui le contiennent. Ce faisceau est bien défini par $h(\infty)$ et un quelconque des cercles qu'il contient, par exemple l'image de la droite de $\mathbb{R}^2$ parallèle à l'axe des abscisses passant par $h^{-1}(\infty)$.

Type hyperbolique. On parle de sous-groupe *de type hyperbolique* lorsque X possède deux valeurs propres réelles non nulles a et $-a$ (la trace de X est nulle). Quitte à remplacer X par $a^{-1}X$, on peut supposer que $a = 1$, de sorte que X est semblable à

$$X_+ = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

L'image de φ_{X_+} dans $\mathrm{PSL}_2(\mathbb{R})$ est formée des homographies $z \mapsto e^{2t}z$ ($t \in \mathbb{R}$). Ses orbites dans $\mathbb{P}^1(\mathbb{C})$ sont ∞, 0 et les demi-droites contenant 0.

Conjuguer X_+ par un élément quelconque de $\mathrm{GL}_2(\mathbb{C})$ a pour effet de conjuguer le sous-groupe à un paramètre par une homographie h quelconque. D'après ce qui précède, les orbites de ce sous-groupe sont les deux points $h(\infty)$ et $h(0)$ et les cercles du faisceau à points bases qu'ils définissent, ou plus exactement les arcs de cercles délimités par les deux points bases.

Bilan

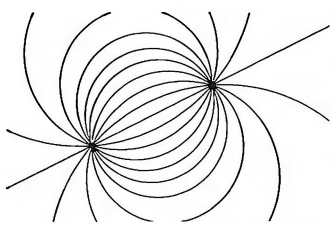
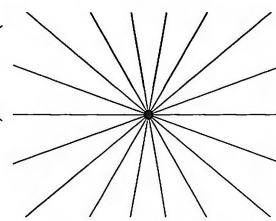
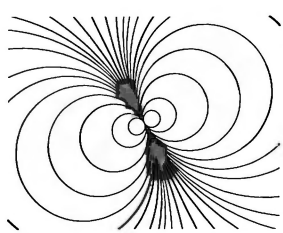
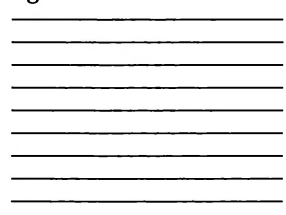
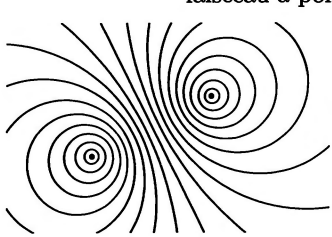
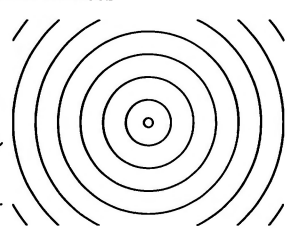
L'application qui, à une homographie $h \in \mathrm{PGL}_2(\mathbb{C})$ et à une matrice non nulle $X \in \mathfrak{sl}_2(\mathbb{R})$ associe le faisceau de cercles de $\mathbb{P}^1$ qui est l'image par h des orbites du sous-groupe à un paramètre φ_X, induit une surjection

$$\mathrm{PGL}_2(\mathbb{C}) \times \mathbb{P}\big(\mathfrak{sl}_2(\mathbb{R})\big) \longrightarrow \mathscr{F}.$$

En réalité, toutes ces constructions viennent de considérations de groupes de Lie : nous sommes implicitement en train de travailler dans l'*espace symétrique* $\mathrm{PGL}_2(\mathbb{C})/\mathrm{PGL}_2(\mathbb{R})$, quotient du groupe par les points fixes de la conjugaison complexe σ. L'algèbre de Lie de $\mathrm{PGL}_2(\mathbb{C})$ s'identifie à $\mathfrak{sl}_2(\mathbb{C})$, elle se décompose en la somme directe de la sous-algèbre $\mathfrak{sl}_2(\mathbb{R})$ (points fixes de σ dans $\mathfrak{sl}_2(\mathbb{C})$) et de l'espace $i\mathfrak{k}$ où $\mathfrak{k}$ est l'espace des matrices hermitiennes de trace nulle (espace propre de σ de valeur propre -1). Quant à l'orthogonalité des faisceaux, son origine est à chercher dans la décomposition d'Iwasawa $\mathrm{SL}_2(\mathbb{R})/K = KAK/K$, où $K = \mathrm{SO}_2(\mathbb{R})$ et A est le sous-groupe des matrices diagonales à coefficients positifs. Les algèbres de Lie de K et de A sont orthogonales pour une forme naturelle, la *forme de Killing*. Et, ainsi de suite.

A. Annexe. Faisceaux et sous-groupes à un paramètre

Comme à l'accoutumée, mais de façon plus imagée, nous voici face à un tableau présentant les orbites pour une action de groupe. Ici, il s'agit de l'action du groupe $\mathrm{PSL}_2(\mathbb{C})$ sur les faisceaux de cercles de $\mathbb{P}^1(\mathbb{C})$ par homographies. La première colonne montre un faisceau typique de l'orbite. Il faut la distinguer de la forme normale, paradoxalement plus atypique[12], mais plus maniable, que l'on trouvera dans la colonne du milieu.

faisceau de cercles		sous-groupe
typique	forme normale	« générateur » X sous-groupe
faisceau à points bases		type hyperbolique
		$X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\varphi_X(t) : z \mapsto e^{2t}z$ $(t \in \mathbb{R})$
faisceau tangent		type parabolique
		$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\varphi_X(t) : z \mapsto z + t$ $(t \in \mathbb{R})$
faisceau à points limites		type elliptique
		$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $\varphi_X(t) : z \mapsto e^{it}z$ $(t \in \mathbb{R})$

[12] C'est un paradoxe parce que le normal devrait être typique, mais nous y sommes habitués — voir par exemple l'alternative de Steiner [H2G2, §XI-3 et figure XI-3.4].

La troisième colonne fait référence à l'interprétation de ces faisceaux que nous venons de faire en terme de sous-groupes à un paramètre de $\mathrm{SL}_2(\mathbb{C})$. Chaque faisceau est l'ensemble des orbites pour l'action naturelle d'un sous-groupe de $\mathrm{SL}_2(\mathbb{C})$ de la forme $\varphi_X(\mathbb{R}) = \{\exp(tX),\ t \in \mathbb{R}\}$ sur $\mathbb{P}^1(\mathbb{C})$, où X désigne une matrice (non nulle) de trace nulle. Si X et X' sont conjuguées, alors les sous-groupes $\varphi_X(\mathbb{R})$ et $\varphi_{X'}(\mathbb{R})$ le sont également. Les faisceaux associés sont alors dans une même orbite.

Notons que sur chaque ligne, les dessins qui paraissent différents dans le plan se mettent à se ressembler énormément lorsqu'on les regarde sur la sphère par une projection stéréographique inverse.

B. Exercices du chapitre VI

B.1. Exercice (Application fraîche et joyeuse de la décomposition polaire)

Voici un exercice dont le charme discret et la simplicité nous feront oublier qu'il n'a pas vraiment sa place ici.

Soit φ un endomorphisme de l'espace euclidien $\mathbb{R}^n$. Soit m un entier entre 1 et $n-1$, on suppose que φ conserve les m-volumes (disons pour faire simple, les volumes des m-parallélépipèdes). On veut montrer que φ est une isométrie.

1. *Montrer que φ est inversible.*

   Sinon, l'endomorphisme φ aurait un noyau non trivial, et l'image d'un m-parallélépipède de m-volume non nul dont une arête appartient au noyau aurait un volume nul.

2. *Soit $\varphi = o\sigma$, où $o \in \mathrm{O}_n(\mathbb{R})$ et $\sigma \in \mathcal{S}_n^{++}(\mathbb{R})$, la décomposition polaire de φ. Montrer que σ conserve les m-volumes.*

   Constater simplement que $\sigma = o^{-1}\varphi$.

3. *Soient $\lambda_1, \dots, \lambda_n$ les valeurs propres de σ. Montrer que pour toute m-suite $1 \leqslant i_1 < \cdots < i_m \leqslant n$, on a : $\prod_{j=1}^m \lambda_{i_j} = 1$.*

   Considérer l'image de tous les m-parallélépipèdes dont les arêtes sont des vecteurs propres de σ. La conservation des m-volumes appliquée à ces parallélépipèdes donne le résultat.

4. *En déduire que σ est l'identité et conclure.*

   Pour tous j, j' entre 1 à n, on peut choisir une partie I à $m-1$ éléments ne contenant ni j, ni j'. On a alors : $\lambda_j \prod_{i\in I} \lambda_i = 1 = \lambda_{j'} \prod_{i\in I} \lambda_i$. Cela donne $\lambda_j = \lambda_{j'}$, d'où tous les λ_i sont égaux à 1. On a donc : $\varphi = o\sigma = o$.

B.2. Exercice (Différentielle de la conjugaison — le retour !)

Soit ad *l'application* adjointe, *c'est-à-dire* $\mathrm{ad} : \mathscr{M}_n(\mathbb{R}) \to \mathrm{End}\big(\mathscr{M}_n(\mathbb{R})\big)$, *qui envoie* X *sur* $\mathrm{ad}(X) = [X, ?]$. *On a vu dans [H2G2, exemples IX-1.4 (v)] que* ad *est la différentielle de la conjugaison en l'identité, la conjugaison étant vue comme application de* $\mathrm{GL}_n(\mathbb{R})$ *dans* $\mathrm{GL}\big(\mathscr{M}_n(\mathbb{R})\big)$. *Il est permis de se demander si l'on peut récupérer la conjugaison à partir de* ad.

Montrer que pour tous X *et* Y *de* $\mathscr{M}_n(\mathbb{R})$, *on a*

$$\exp\big(\mathrm{ad}(X)\big)(Y) = \exp(X) Y \exp(X)^{-1}.$$

On écrit $\exp(X)^{-1} = \exp(-X)$, et le reste est juste un peu de calcul formel.

Pfaffiens

B.3. Exercice. *Montrer que les groupes* $\mathrm{SL}_4(\mathbb{R})/\{\mathrm{Id}, -\mathrm{Id}\}$ *et* $\mathrm{SO}_0(3,3)$ *sont isomorphes et que* $\mathrm{SL}_4(\mathbb{F}_q)/\{\mathrm{Id}, -\mathrm{Id}\}$ *est isomorphe à un sous-groupe d'indice* 2 *de* SO_6^ζ, *avec* $\zeta = -1$.

Sur $\mathbb{R}$, on pourra suivre la preuve du théorème 2.12, en calculant la signature du pfaffien. Sur $\mathbb{F}_q$, on pourra remplacer l'argument de géométrie différentielle par un argument de cardinalité qui utilise le théorème IV-2.1.

B.4. Exercice (Pfaffien)

Soit $\mathbb{K}$ *un corps de caractéristique différente de* 2 *et soit* $A = (a_{ij}) \in \mathscr{A}_{2m}$, *où* $\mathscr{A}_{2m}$ *est le sous-espace des matrices antisymétriques de* $\mathscr{M}_{2m}(\mathbb{K})$. *On note* σ_A *la forme bilinéaire antisymétrique associée à* A *dans la base canonique* (e_i) *de* $\mathbb{K}^{2m}$. *On considère la forme* ω_A *définie par*

$$\omega_A : \big(\mathbb{K}^{2m}\big)^{2m} \to \mathbb{K}, \quad (v_1, \ldots, v_{2m}) \mapsto \frac{1}{2^m m!} \sum_{\pi \in \mathfrak{S}_{2m}} \varepsilon(\pi) \prod_{i=1}^{m} \sigma_A\big(v_{\pi(2i-1)}, v_{\pi(2i)}\big),$$

où $\mathfrak{S}_{2m}$ *est le groupe symétrique et* ε *désigne la signature.*

1. *Montrer que* ω_A *est une forme* $2m$*-linéaire alternée et en déduire l'existence d'une fonction* $\mathrm{Pf} : \mathscr{A}_{2m} \to \mathbb{K}$ *telle que pour tout* A, *on ait :* $\omega_A = \mathrm{Pf}(A) \det$. *Cette fonction est appelée* pfaffien.

   On montre qu'elle est alternée par le changement de variable $\pi' = \pi \circ s$, où s est une permutation. L'égalité provient de l'unicité d'une telle forme à scalaire près.

2. *En évaluant cette formule sur la base canonique de* $\mathbb{K}^{2m}$, *montrer*

$$\mathrm{Pf}(A) = \frac{1}{2^m m!} \sum_{\pi \in \mathfrak{S}_{2m}} \varepsilon(\pi) \prod_{i=1}^{m} a_{\pi(2i-1), \pi(2i)}.$$

3. *Montrer l'égalité* $\sigma_A(Pu, Pv) = \sigma_{{}^tPAP}(u, v)$, *pour toute matrice* P *et tout couple* (u, v) *de* $\mathbb{K}^{2m}$. *En déduire*

$$\mathrm{Pf}({}^tPAP) = \mathrm{Pf}(A)\det(P).$$

4. *Montrer que si* $\det(A) = 0$, *alors* $\mathrm{Pf}(A) = 0$.
On pourra appliquer la formule du pfaffien à une base $(v_1, \ldots, v_{2m})$ contenant une base du noyau de σ_A.

5. *(a) On pose* $J_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *et* $J_m = \begin{pmatrix} J_1 & 0 & & 0 \\ 0 & J_1 & & 0 \\ \vdots & \vdots & & \vdots \\ 0 & \ldots & \ldots & J_1 \end{pmatrix}$.

Établir que $\sigma_{J_m}(e_{\pi(2i-1)}, e_{\pi(2i)}) \neq 0$ *si et seulement si* π *permute les sous-ensembles* $\{2i-1, 2i\}$ *(pour* $1 \leqslant i \leqslant m$*) et que dans ce cas, on a :* $\sigma_{J_m}(e_{\pi(2i-1)}, e_{\pi(2i)}) = \varepsilon(\pi)$ *pour tout* i.

(b) En déduire que l'on a : $\mathrm{Pf}(J_m) = 1$.

(c) Montrer que si σ_A *est non dégénérée, alors* $\mathrm{Pf}(A)^2 = \det(A)$.
On a les égalités $\mathrm{Pf}(A) = \det(P)$, d'une part, et $\det(A) = \det(P)^2$, d'autre part.

6. *Montrer que pour toute matrice* A, $\mathrm{Pf}(A)^2 = \det(A)$.
L'égalité est vraie dans les deux cas, selon que A est dégénérée ou non.

Isomorphismes exceptionnels

B.5. Exercice (Sous-espaces de matrices diagonalisables)

On considère l'espace vectoriel $\mathscr{M}_2(\mathbb{R})$. *Le but de l'exercice est de montrer, en utilisant un isomorphisme exceptionnel, que tout sous-espace maximal constitué de matrices diagonalisables est conjugué à l'espace des matrices symétriques. On note* H *l'hyperplan des matrices de trace nulle.*

1. *Montrer qu'une matrice non nulle* A *de* H *est diagonalisable si et seulement si son déterminant est strictement négatif.*

2. *On rappelle ([H2G2, proposition IX-2.3]) que l'action par conjugaison de* $\mathrm{SL}_2(\mathbb{R})$ *sur* H *définit un isomorphisme de* $\mathrm{PSL}_2(\mathbb{R})$ *sur* $\mathrm{SO}_0(2,1)$. *Résoudre alors le problème posé en commençant par se ramener au problème analogue dans* H.
Sur H, la forme $-\det$ est de signature $(2,1)$ et toutes les grassmanniennes de signature $(2,1)$ sont dans la même $\mathrm{SO}_0(2,1)$-orbite. Le problème est résolu sur H, et l'on généralise en disant que la droite des homothéties est un supplémentaire de H.

B.6. Exercice (Plongement de Segre)

Soit $\mathbb{K}$ un corps quelconque. On considère l'application

$$\sigma : \mathbb{P}^n(\mathbb{K}) \times \mathbb{P}^m(\mathbb{K}) \to \mathbb{P}^{(n+1)(m+1)-1}(\mathbb{K}),$$

$$\big([x_0 : \cdots : x_n], [y_0 : \cdots : y_m]\big) \mapsto [x_0y_0 : x_0y_1 : \cdots : x_0y_m : x_1y_0 : \cdots : x_ny_m].$$

On notera $\big[(z_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m}\big]$ un élément de $\mathbb{P}^{(n+1)(m+1)-1}$, où les coordonnées z_{ij} sont placées dans l'ordre lexicographique.

1. *Montrer que σ est bien définie et qu'elle est injective.*
2. *Montrer que l'image de σ est la quadrique $\big\{[z_{ij}],\ z_{ij}z_{kl} = z_{il}z_{kj}\big\}$.*
   On pourra écrire $[z_{ij}]$ par colonnes comme la classe d'une matrice dans $\mathbb{P}\mathscr{M}_{m+1,n+1}$, puis voir que la condition quadratique imposée est équivalente à dire que la matrice est de rang 1.
3. *Montrer que si $n = m = 1$, on retrouve l'application α de la proposition 2.6.*

Formes symplectiques et lagrangiens

B.7. Exercice (Lagrangiens sur un corps quelconque)

Ici, $\mathbb{K}$ est un corps quelconque de caractéristique différente de 2. On considère la forme antisymétrique ω sur $\mathbb{K}^{2n}$ donnée par

$$\omega\big((x_1, \ldots, x_n, y_1, \ldots, y_n), (x'_1, \ldots, x'_n, y'_1, \ldots, y'_n)\big) = \sum\nolimits_k x_k y'_k - y_k x'_k.$$

Par [H2G2, proposition V-4.1], à changement de base près, toute forme antisymétrique non dégénérée sur $\mathbb{K}^{2n}$ peut s'écrire ainsi. On note $\mathrm{Sp}_{2n}(\mathbb{K})$ le sous-groupe de $\mathrm{GL}_{2n}(\mathbb{K})$ qui stabilise la forme ω. Pour tout sous-espace K, on notera $K^\perp$ son orthogonal pour ω.

1. *Soit K un sous-espace de $\mathbb{K}^{2n}$ tel que la restriction de ω à $K \times K$ soit nulle. Montrer que K est inclus dans son orthogonal $K^\perp$ pour ω. En déduire que sa dimension vérifie $\dim K \leqslant n$. On appelle* lagrangien *un sous-espace L de $\mathbb{R}^{2n}$ de dimension n tel que $\omega|_{L\times L}$ soit nulle.*
2. *Montrer que tout sous-espace K de $\mathbb{K}^{2n}$ tel que la restriction de ω à $K \times K$ soit nulle est contenu dans un lagrangien.*
   On a par hypothèse $K \subset K^\perp$. Si l'on a égalité, alors K est un lagrangien. Sinon, on peut trouver un vecteur v dans le complémentaire de K dans $K^\perp$. On considère alors le sous-espace $K \oplus \langle v\rangle$ sur lequel ω est nulle, et l'on achève à l'aide d'une récurrence finie.
3. *On fixe K comme dans la question précédente.*
   (a) *Montrer qu'il existe une base $\mathbf{f} = (f_1, \ldots, f_n, f_{n+1}, \ldots, f_{2n})$, de $\mathbb{K}^{2n}$ telle que $(f_1, \ldots, f_n)$ soit une base de K et que ω s'écrive $\left(\begin{smallmatrix} 0_n & I_n \\ -I_n & 0_n \end{smallmatrix}\right)$ dans la base $\mathbf{f}$.*

On commence par f_1 non nul dans K, puis f_{n+1} dans le complémentaire $\langle f_1\rangle^\perp$. Par récurrence finie sur j, tant que $j < n$, on construit f_{j+1} non nul dans $K \cap \langle f_{n+1}, \dots, f_{n+j}\rangle^\perp$, puis f_{n+j+1} dans le complémentaire de $\langle f_1, \dots, f_j, f_{j+1}, f_{n+1}, \dots, f_{n+j}\rangle^\perp$ dans $\langle f_1, \dots, f_j, f_{n+1}, \dots, f_{n+j}\rangle^\perp$. On montre par des arguments de dimension et par la formule de Grassmann que ces éléments ainsi construits existent bel et bien.

(b) En déduire que $\mathrm{Sp}_{2n}(\mathbb{K})$ *agit transitivement sur l'ensemble des lagrangiens.*

B.8. Exercice (Espace des lagrangiens sur $\mathbb{R}^{2n}$)

Tout au long de cet exercice, on identifiera les $\mathbb{R}$*-espaces* $\mathbb{C}^n$ *et* $\mathbb{R}^{2n}$ *via l'application* $(z_k) \mapsto (x_1, \dots, x_n, y_1, \dots, y_n)$*, où* x_k *et* y_k *sont respectivement les parties réelle et imaginaire de* z_k*.*

On considère sur $\mathbb{C}^n$ *la forme*

$$\omega(z, z') = \sum_k x_k y'_k - y_k x'_k\,.$$

1. *Montrer que la* $\mathbb{R}$*-forme* ω *est antisymétrique et non dégénérée sur* $\mathbb{R}^{2n}$*.*
2. *Soit* L *un* $\mathbb{R}$*-sous-espace de* $\mathbb{R}^{2n}$ *tel que la restriction de* ω *à* $L \times L$ *soit nulle. Montrer que* L *est inclus dans son orthogonal* $L^\perp$ *pour* ω*. En déduire que sa dimension (réelle) vérifie* $\dim L \leqslant n$*. On appelle* lagrangien *un sous-espace de* $\mathbb{R}^{2n}$ *de dimension* n *tel que* $\omega|_{L\times L}$ *soit nulle.*
3. *On munit* $\mathbb{C}^n$ *de la forme hermitienne* $h(z, z') = \sum_k \bar{z}_k z'_k$*. Montrer que la décomposition cartésienne de* $h(z, z')$ *est*

$$h(z, z') = \varphi(z, z') + i\omega(z, z'),$$

où φ *est la forme euclidienne canonique de* $\mathbb{R}^{2n}$*. En déduire que le plongement naturel de* $\mathbb{R}^n$ *dans* $\mathbb{C}^n$ *(via* $(x_k) \mapsto (x_k + 0i)$*) fournit un lagrangien de* $\mathbb{R}^{2n}$*. Par la suite, on notera* L_0 *ce lagrangien.*

4. *(a) Montrer que si* L *est un* $\mathbb{R}$*-sous-espace vectoriel de* $\mathbb{C}^n$ *tel que* $h_L = h|_{L\times L}$ *soit une forme réelle (*i.e. *son image est dans* $\mathbb{R}$*), alors* h_L *est symétrique définie positive.*

   (b) En déduire que $\mathrm{U}(n)$ *agit transitivement sur l'ensemble* $\mathscr{L}$ *des lagrangiens de* $\mathbb{R}^{2n}$*.*
5. *Montrer que le stabilisateur de* L_0 *pour cette action est isomorphe à* $\mathrm{O}(n)$ *et que l'on a alors une bijection* $\mathscr{L} \simeq \mathrm{U}(n)/\mathrm{O}(n)$*.*
6. *Montrer que l'espace* $\mathscr{L}$*, muni de la topologie obtenue par transport de structure, est compact et connexe.*

B.9. Exercice (Orbites coadjointes)

Soit $G = \mathrm{GL}_n(\mathbb{R})$ et soit $\mathfrak{g} = \mathscr{M}_n(\mathbb{R})$ son algèbre de Lie.

1. *Montrer que $(A, B) \mapsto \mathrm{tr}(AB)$ définit une forme bilinéaire symétrique non dégénérée sur $\mathfrak{g}$.*

   Voir [H2G2, exercice V-D.3]

2. *En déduire un isomorphisme τ de $\mathfrak{g}$ dans le dual $\mathfrak{g}^*$, qui envoie la matrice A sur la forme linéaire $\big(B \mapsto \mathrm{tr}(AB)\big) \in \mathfrak{g}^*$.*

3. *On fait agir[13] G sur $\mathfrak{g}$ par l'action adjointe et sur $\mathfrak{g}^*$ par $g \cdot \varphi = \varphi(g^{-1}?g)$. Montrer que l'isomorphisme τ commute à l'action de G.*

   C'est juste la formule $\mathrm{tr}(AP^{-1}BP) = \mathrm{tr}(PAP^{-1}B)$.

4. *Soit φ dans $\mathfrak{g}^*$ et soit G_φ son stabilisateur dans G. Montrer que G_φ est un groupe de Lie et que son algèbre de Lie est :*

$$\mathfrak{g}_\varphi = \{X \in \mathfrak{g},\ \forall Y \in \mathfrak{g},\ \varphi(XY - YX) = 0\}.$$

   On pourra s'inspirer de la preuve du corollaire III-6.6. Autre méthode : pour le groupe de Lie, invoquer le théorème de Cartan ([60, §3.4]) et pour l'algèbre de Lie, une inclusion est évidente et l'autre peut se voir par l'exercice B.2.

5. *Montrer que $\omega : (X, Y) \mapsto \varphi(XY - YX)$ définit une forme bilinéaire antisymétrique sur $\mathfrak{g}$ et que son noyau est $\mathfrak{g}_\varphi$.*

6. *En déduire que la codimension de $\mathfrak{g}_\varphi$ est paire et donc, en posant $u = \tau^{-1}(\varphi)$, que la codimension du commutant d'un endomorphisme u de $\mathfrak{g}$ est paire.*

   Comme τ est un isomorphisme G-invariant, le stabilisateur G_φ est égal au stabilisateur G_u pour l'action adjointe, et donc, son algèbre de Lie $\mathfrak{g}_u$, qui est aussi le commutant de u, est égale à $\mathfrak{g}_\varphi$.

On retrouve ainsi le corollaire II-2.9 mais par une méthode constructive plutôt que comptable : il prend corps dans les variétés symplectiques. Sans vouloir trop rentrer dans les détails, l'orthogonal du noyau $\mathfrak{g}_\varphi$ dans $\mathfrak{g}^*$ est alors naturellement[14] muni d'une forme bilinéaire symplectique. Or, cet orthogonal est l'espace tangent en φ à l'orbite coadjointe de φ. L'action de G fournit, par translation, une structure dite symplectique sur toute l'orbite. Cette idée simple, due à des mathématiciens comme Felix Berezin, Alexandre A. Kirillov, Bertram Kostant ou Jean-Marie Souriau, a permis de fabriquer une machine puissante pour, d'une part, produire des représentations (par la « méthode des orbites »), d'autre part, trouver des systèmes intégrables.

[13] Cette action est appelée action coadjointe.

[14] L'orthogonal de $\mathfrak{g}_\varphi$ dans le dual s'identifie à $\mathfrak{g}/\mathfrak{g}_\varphi$, sur lequel la forme ω définit une forme bilinéaire antisymétrique non dégénérée.

Simplicité des groupes orthogonaux

B.10. Exercice (Simplicité de $\mathrm{SO}(2n+1)$)

Le but de l'exercice est de démontrer que le groupe $\mathrm{SO}(2n+1)$ *ne possède pas de sous-groupe distingué non trivial. Soit donc* H *un sous-groupe distingué de* $\mathrm{SO}(2n+1)$ *et soit* $h \in H$, $h \neq \mathrm{Id}$. *Le but est donc d'établir que* $H = \mathrm{SO}(2n+1)$. *On munit l'espace* $\mathbb{R}^{2n+1}$ *de sa structure canonique d'espace euclidien et l'on note* $(e_i)_{1 \leqslant i \leqslant 2n+1}$ *sa base orthonormée canonique.*

1. *Montrer que* 1 *est valeur propre de* h. *Dans la suite, on notera* $k > 0$ *la dimension du sous-espace propre* E_1 *associé.*

   Les valeurs propres sont 1, -1, ou des valeurs propres conjuguées, λ, $\bar{\lambda}$, telles que $\lambda\bar{\lambda} = 1$. On utilise la parité et le fait que leur produit vaut $\det(h) = 1$.

2. *Soit* $(f_1, \ldots, f_k, \ldots, f_{2n+1})$ *une base orthonormée de* $\mathbb{R}^{2n+1}$ *telle que la famille* $(f_1, \ldots, f_k)$ *est une base de* E_1. *Montrer que pour toute partie* I *à* k *éléments de* $[1, 2n+1]$, *il existe* ρ_I *dans* $\mathrm{SO}(2n+1)$ *qui envoie* $(f_1, \ldots, f_k)$ *dans* $(e_i)_{i \in I}$.

   L'existence dans $\mathrm{O}(2n+1)$ est claire ; pour trouver ρ_I dans $\mathrm{SO}(2n+1)$, il faut utiliser le fait que $k < 2n+1$, c'est-à-dire que h n'est pas l'identité.

3. *Pour toute partie* I *à* k *éléments, on pose donc* $h_I = \rho_I \circ h \circ \rho_I^{-1} \in H$; *soit alors* $\phi : \mathrm{SO}(2n+1) \to \mathrm{SO}(2n+1)$ *telle que* $\phi(g) = \prod_I g h_I g^{-1} h_I^{-1}$, *(on aura fixé un ordre sur l'ensemble des parties à* k *éléments de l'intervalle* $[1, 2n+1] \subset \mathbb{N}$*). Montrer que* ϕ *est différentiable et que la différentielle en l'identité de* ϕ *est donnée par* $\mathrm{d}_e\phi(A) = KA - \sum_I h_I A h_I^{-1}$, *pour tout* A *dans* $\mathfrak{so}_{2n+1}$, *en posant* $K = \binom{2n+1}{k}$.

4. *Soit* A *une matrice de* $\ker \mathrm{d}_e\phi$. *On note* q *la norme matricielle quadratique* $q(M) = \mathrm{tr}({}^tMM)$, *voir [H2G2, exercice V-D.3].*

   (a) Montrer que l'on a :

   $$\frac{1}{K}\sum_I q(h_I A h_I^{-1}) = q(A) = q\Big(\frac{1}{K}\sum_I h_I A h_I^{-1}\Big).$$

   Une fois montré que $q(h_I A h_I^{-1}) = q(A)$, c'est tout droit !

   (b) Montrer que $h_I A h_I^{-1} = A$ *pour tout* I.

   La convexité stricte est toujours vérifiée pour une forme définie positive. On peut aussi remarquer la formule

   $$m\sum_{i=1}^m q(v_i) - q\Big(\sum_{i=1}^m v_i\Big) = \sum_{1 \leqslant i < j \leqslant m} q(v_i - v_j).$$

   (c) En déduire que A *est diagonalisable, puis, que* $A = 0$.

   Pour tout I, A stabilise donc le sous-espace propre de h_I pour la valeur propre 1, c'est-à-dire que A stabilise $\rho_I(E_1)$. Or, comme

$k < 2n+1$, chaque droite $\mathbb{R}e_i$ peut être réalisée comme intersection d'une famille de $\rho_I(E_1)$. Donc, chaque droite $\mathbb{R}e_i$ est stable par A et donc A est diagonalisable sur $\mathbb{R}$. Comme A est antisymétrique, ses valeurs propres sont nulles.

(d) Conclure que $H = \mathrm{SO}(2n+1)$.

On a vu que la différentielle $\mathrm{d}_e\phi$ de ϕ en e était injective : elle est donc iso. Comme dans [H2G2, §IX-2], on applique le théorème d'inversion locale pour montrer que l'image contient un ouvert. Comme l'image est contenue dans H (car H est distingué), on a par le principe de translation que H est ouvert (et donc fermé). La connexité de $\mathrm{SO}(2n+1)$ permet de conclure que $H = \mathrm{SO}(2n+1)$.

B.11. Exercice (Simplicité de PSO(2n), $n \geqslant 3$)

Le groupe spécial orthogonal $\mathrm{SO}(2n)$ *ne peut être simple puisqu'il possède un centre non trivial* $Z = \{\pm \mathrm{Id}\}$. *On sait de par ailleurs que le groupe* $\mathrm{PSO}(4)$ *n'est pas simple ([H2G2, §VII-4]). Nous allons montrer que* $\mathrm{PSO}(2n)$ *est simple pour* $n \geqslant 3$, *ce qui, avec l'exercice ci-dessus, prouvera la simplicité de tous les groupes* $\mathrm{PSO}(n)$ *sur* $\mathbb{R}$, *à l'exception des cas* $n = 2, 4$. *On se donne donne donc un sous-groupe distingué* H *non trivial de* $\mathrm{PSO}(2n)$ *et l'on veut montrer qu'il est égal à* $\mathrm{PSO}(2n)$. *On munit l'espace* $\mathbb{R}^{2n}$ *de sa structure euclidienne canonique.*

1. *Soit* ϖ *la projection canonique de* $\mathrm{SO}(2n)$ *sur* $\mathrm{PSO}(2n)$. *Soit* $\tilde{H} = \varpi^{-1}(H)$ *et soit* $s \neq \pm \mathrm{Id}$ *dans* $\tilde{H}$. *Montrer qu'il existe un plan* P *de* $\mathbb{R}^{2n}$, *non fixé par* s.

   Comme $n \geqslant 2$, toute droite peut être réalisée comme intersection de deux plans. Si s fixait tous les plans, il fixerait toutes les droites et il serait central. Or, $s \neq \pm \mathrm{Id}$ assure qu'il n'est pas central.

2. *Soit* r *un retournement de* $\mathrm{SO}(2n)$ *par rapport à* P. *Montrer que* $h = rsr^{-1}s^{-1}$ *est un élément de* $\tilde{H}$ *dont* 1 *est valeur propre et tel que* $h \neq \mathrm{Id}$.

   Le sous-groupe $\tilde{H}$ étant distingué, h est le produit de deux éléments de $\tilde{H}$, nommément, rsr^{-1} et s^{-1} donc dans $\tilde{H}$. De plus, c'est un produit de deux retournements, en l'occurrence r par rapport à P et $sr^{-1}s^{-1}$ par rapport à un plan Q. Donc, h vaut l'identité sur le sous-espace $P^\perp \cap Q^\perp$, lequel est de dimension $\geqslant 1$, car $n \geqslant 3$. Pour finir, comme s ne stabilise pas P, r et s ne commutent pas, et donc $h \neq \mathrm{Id}$.

3. *Montrer à l'aide de l'exercice ci-dessus que* $\tilde{H} = \mathrm{SO}(2n)$ *et conclure.*

   Il suffit de suivre l'exercice B.10 avec l'élément h ainsi construit. La conclusion est immédiate, car ϖ est surjective !

« Dites-moi, Annie, fit-il en tirant quelques feuillets de sa serviette, on ne vous a jamais dit que le point-virgule était mort ? »

Philippe Djian, *Incidences*, 2010.
Cité par Arnaud & Jean-Marie Larrieu, *L'amour est un crime parfait* 2013.

Chapitre VII

Droite projective et birapport

Ce chapitre est un éloge et une glorification du birapport. Invariant d'une symétrie, en l'occurrence l'homographie de la droite projective, il se prête à l'étude des symétries de l'invariant ; surgit alors l'invariant modulaire — l'invariant j pour les intimes — et c'est vers les courbes elliptiques que conduit ce chemin jalonné de pépites. Dans une autre direction plus géométrique, le birapport est un lien naturel entre deux types de modèles du plan hyperbolique : le demi-plan de Poincaré et le disque de Klein. C'est amusant, car on voit interagir deux métriques aux saveurs différentes, deux géométries projectives au fond, celle de la droite complexe et celle du plan réel. Dans les deux, on trouve le groupe $\mathrm{PSL}_2(\mathbb{R})$ des isométries du plan hyperbolique. Puis, l'action des homographies sur ce dernier met en évidence des sous-groupes remarquables — libres — du groupe $\mathrm{PSL}_2(\mathbb{Z})$, que l'on exploite pour mettre une structure d'arbre sur les triplets pythagoriciens. Enfin, après les fractions rationnelles, les réels et les complexes, on passe une nouvelle fois dans des corps finis où le birapport explique plusieurs isomorphismes exceptionnels déjà rencontrés.

Oui, le birapport est bien, avec l'algorithme de Gauss, le deuxième œil qui permet d'appréhender l'univers.

1. Birapport, équation de degré 4 et interprétations géométriques

Avant tout, rappelons un peu comment construire, de façon un peu convaincante, le birapport. Tout d'abord, qu'est-ce que le rapport ? Considérons

la droite affine $\mathbb{A}^1(\mathbb{K})$ sur un corps $\mathbb{K}$ et sur laquelle agit le groupe affine $\mathrm{GA}_1(\mathbb{K})$ par $z \mapsto az + b$ ($a \in \mathbb{K}^*$, $b \in \mathbb{K}$). L'action est deux fois simplement transitive ([H2G2, définition I-A.1.9]), puisque par deux points distincts passe une droite et une seule (Euclide!). Selon une logique « erlanguienne » bien rodée, déjà formulée en [H2G2, remarque X-1.2.12], il faut faire agir le groupe $\mathrm{GA}^1(\mathbb{K})$ sur trois points (z_1, z_2, z_3), deux à deux distincts, pour obtenir un invariant intéressant. Il s'agit bien entendu du rapport $(z_3 - z_1)/(z_3 - z_2)$ que l'on retrouve aussi bien bien dans le théorème de Thalès, dans les mesures d'angles et de distances que dans les problèmes de règle de trois ou de pourcentages, qui ont fait les beaux jours du certificat d'étude.

Considèrons maintenant la droite projective $\mathbb{P}^1(\mathbb{K})$ (l'ensemble des droites du plan vectoriel assimilé à $\mathbb{A}^1(\mathbb{K}) \cup \{\infty\}$, le point « infini » étant vu comme la droite « verticale »), sur laquelle agit le groupe $\mathrm{PGL}_2(\mathbb{K})$ par $z \mapsto (az + b)/(cz + d)$. Alors, l'action est trois fois simplement transitive par [H2G2, proposition X-1.2.7], et ainsi, l'action sur un quadruplet (z_1, z_2, z_3, z_4) fournit un nouvel invariant géométrique, le fameux birapport. On note pour cela que le rapport $(z_3 - z_1)/(z_3 - z_2)$ cité au-dessus, est envoyé sur $\alpha(z_3 - z_1)/(z_3 - z_2)$, où $\alpha = (cz_2 + d)/(cz_1 + d)$, qui n'est certes pas trivial mais qui ne dépend plus que de z_1 et z_2. Pour éliminer α, il faut donc le quotienter par un autre rapport, d'où la notion de birapport[1] :

$$\frac{z_3 - z_1}{z_3 - z_2} : \frac{z_4 - z_1}{z_4 - z_2}.$$

Et c'est là que commence notre histoire (hédoniste).

Dans le calcul des valeurs possibles du birapport de quatre points dans [H2G2, lemme X-1.2.18], on a vu le birapport comme une fraction rationnelle en $z_1, \ldots, z_4$ qui présente certaines symétries par rapport à $\mathfrak{S}_4$, le groupe de Klein ou le quotient $\mathfrak{S}_3$. Il est tentant d'introduire l'équation « générique » dont les z_k sont les racines et de voir le groupe symétrique comme un groupe de Galois.

Le birapport apparaît alors comme un générateur du corps fixé par le groupe de Klein. En poursuivant l'étude par le calcul du polynôme minimal du birapport, on voit apparaître une fraction rationnelle intéressante, notée j, qui, en définitive, permet de classer les quadruplets de points de $\mathbb{P}^1$ quand on oublie l'ordre.

Par commodité, on reste en caractéristique zéro, ce qui assure automatiquement la séparabilité. On commence avec le corps des fractions rationnelles à coefficients rationnels puis l'on spécialise les indéterminées en des nombres complexes.

[1] Bob Marley pensait-il au birapport en écrivant : "Baby, you're so nice, I'd like to do the same thing twice" ?

1.1. Fractions invariantes sous le groupe de Klein

Soit $\mathbb{L} = \mathbb{Q}(z_1, z_2, z_3, z_4)$ le corps des fractions rationnelles en quatre indéterminées. Le groupe symétrique $\mathfrak{S}_4$ agit sur $\mathbb{L}$ par permutation des indéterminées, de même que le sous-groupe distingué engendré par les double-transpositions appelé *groupe de Klein* :

$$\mathfrak{K} = \{e, (12)(34), (13)(24), (14)(23)\}.$$

Soit $\mathbb{K} = \mathbb{L}^{\mathfrak{S}_4}$ le corps fixe : c'est le corps des fractions rationnelles en les polynômes symétriques élémentaires σ_k, où, pour $1 \leqslant k \leqslant 4$:

$$\sigma_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant 4} z_{i_1} \cdots z_{i_k}.$$

On va voir que l'extension intermédiaire $\mathbb{L}^{\mathfrak{K}}$ est intimement liée au birapport. On commence par quelques éléments du [H2G2, X-1.2.13, X-1.2.18 et X-1.2.20], que l'on interprète en termes de fractions rationnelles.

1.2. Définition. Le *birapport* est la fraction rationnelle

$$\lambda = [z_1, z_2, z_3, z_4] = \frac{z_3 - z_1}{z_3 - z_2} \times \frac{z_4 - z_2}{z_4 - z_1} \in \mathbb{L}.$$

1.3. Proposition.

(i) *Le groupe symétrique $\mathfrak{S}_4$ est le produit semi-direct du sous-groupe $\mathfrak{S}_3$ (agissant sur $\{1,2,3\}$) et du sous-groupe normal $\mathfrak{K}$.*

(ii) *Le birapport λ est invariant par le groupe de Klein $\mathfrak{K}$.*

(iii) *L'orbite de λ sous le groupe symétrique $\mathfrak{S}_3 \simeq \mathfrak{S}_4/\mathfrak{K}$ est :*

$$e \cdot \lambda = \lambda, \qquad (123) \cdot \lambda = \frac{\lambda - 1}{\lambda}, \quad (132) \cdot \lambda = \frac{-1}{\lambda - 1}$$
$$(12) \cdot \lambda = \frac{1}{\lambda}, \qquad (23) \cdot \lambda = 1 - \lambda, \qquad (13) \cdot \lambda = \frac{\lambda}{\lambda - 1}.$$

La proposition suivante fait apparaître les six valeurs de l'orbite de λ comme l'effet de l'action du groupe de Galois de $\mathbb{L}/\mathbb{K}$ sur l'une d'entre elles.

1.4. Proposition. *L'extension $\mathbb{L}/\mathbb{K}$ est galoisienne de groupe de Galois $\mathfrak{S}_4$. Le birapport engendre le corps $\mathbb{L}^{\mathfrak{K}}$ fixé par le groupe de Klein, soit $\mathbb{L}^{\mathfrak{K}} = \mathbb{K}(\lambda)$. De plus, l'extension $\mathbb{K}(\lambda)/\mathbb{K}$ est galoisienne de groupe de Galois $\mathfrak{S}_3$.*

Démonstration. D'abord, les extensions sont séparables, car la caractéristique de $\mathbb{K}$ est nulle. L'extension $\mathbb{L}/\mathbb{K}$ est normale, car $\mathbb{L}$ est le corps de décomposition du polynôme $f = \prod_{i=1}^{4}(X - z_i) = X^4 + \sum_{k=1}^{4}(-1)^k \sigma_k X^{n-k}$ sur $\mathbb{K}$.

Comme le birapport λ est fixe par $\mathfrak{K}$, on a : $\mathbb{K}(\lambda) \subset \mathbb{L}^{\mathfrak{K}}$. Comme l'orbite de λ sous $\mathfrak{S}_4$ est formée de six valeurs, on sait que $[\mathbb{K}(\lambda) : \mathbb{K}] = 6$. En effet, cela signifie que le polynôme f est irréductible, puisque le groupe de Galois agit transitivement sur ses racines, si bien que le degré du corps de rupture $\mathbb{K}(\lambda)$ de f est égal au degré de f. Comme 6 est justement l'indice du groupe de Klein dans $\mathfrak{S}_4$, il vient :

$$[\mathbb{K}(\lambda) : \mathbb{K}] = 6 = [\mathfrak{S}_4 : \mathfrak{K}] = [\mathbb{L}^{\mathfrak{K}} : \mathbb{K}],$$

d'où l'égalité de $\mathbb{K}(\lambda)$ et $\mathbb{L}^{\mathfrak{K}}$ (et le stabilisateur de λ dans $\mathfrak{S}_4$ est $\mathfrak{K}$).

Enfin, comme $\mathfrak{K}$ est distingué dans $\mathfrak{S}_4$, l'extension $\mathbb{L}^{\mathfrak{K}}/\mathbb{K}$ est galoisienne et son groupe de Galois est : $\mathfrak{S}_4/\mathfrak{K} \simeq \mathfrak{S}_3$. □

On peut jouer un peu, par exemple à calculer le polynôme minimal du birapport λ sur $\mathbb{K}$; cela permet de le relier à l'« invariant modulaire ».

1.5. Lemme. *Le polynôme minimal, sur* $\mathbb{K}$*, du birapport* $\lambda \in \mathbb{L}$ *est :*

$$P(X) = X^6 - 3X^5 + (6-j)X^4 + (2j-7)X^3 + (6-j)X^2 - 3X + 1,$$

où

$$j = \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \in \mathbb{K}.$$

Démonstration. On sait que P a pour racines les conjugués de λ sous le groupe de Galois de l'extension, c'est-à-dire les six homographies de $\mathfrak{S}_3$, ce qui donne :

$$P = (X-\lambda)\big(X - \frac{\lambda-1}{\lambda}\big)\big(X + \frac{1}{\lambda-1}\big)\big(X - \frac{1}{\lambda}\big)\big(X + \lambda - 1\big)\big(X - \frac{\lambda}{\lambda-1}\big).$$

A priori, P appartient à $\mathbb{L}[X]$. Comme le produit porte sur tous les conjugués de λ par le groupe de Galois, les coefficients de P sont dans $\mathbb{K}$. On les calcule en développant :

$$P = X^6 - c_1X^5 + c_2X^4 - c_3X^3 + c_4X^2 - c_5x + c_6,$$

avec $c_6 = 1$, $c_1 = c_5 = 3$ et :

$$c_2 = c_4 = -\frac{\lambda^6 - 3\lambda^5 + 5\lambda^3 - 3\lambda + 1}{\lambda^2(\lambda-1)^2},$$

$$c_3 = -\frac{2\lambda^6 - 6\lambda^5 + 5\lambda^4 + 5\lambda^2 - 6\lambda + 2}{\lambda^2(\lambda-1)^2}.$$

Ces deux relations sont deux équations de degré 6 à coefficients dans $\mathbb{K}$, dont λ est solution : comme P, de degré 6 est le polynôme minimal de λ, elles sont proportionnelles ! De façon plus élémentaire, la ressemblance

entre c_2 et c_3 incite à calculer :

$$c_3 - 2c_2 = -\frac{5\lambda^4 - 10\lambda^3 + 5\lambda^2}{\lambda^2(\lambda-1)^2} = -5.$$

Aussi, le polynôme minimal de λ est :

$$P(X) = X^6 - 3X^5 + c_2X^4 - (2c_2 - 5)X^3 + c_2X^2 - 3X + 1.$$

L'idée est de remplacer c_2 par une autre fraction qui décrit mieux les valeurs où le birapport a moins de six conjugués. Le coefficient c_2 est une fraction en λ. Lorsque l'on spécialise λ en un nombre complexe différent de 0 et 1, cela définit une valeur complexe de $c_2 = c_2(\lambda)$. Connaissant les racines de P, considéré à présent comme un élément de $\mathbb{C}[X]$, on peut affirmer que P a des racines multiples si et seulement si λ est l'une des valeurs suivantes : -1, 2, $1/2$ d'une part, $e^{\pm i\pi/3}$ d'autre part. Si l'on remplace ces valeurs dans l'expression de c_2 en fonction de λ, on trouve respectivement :

$$c_2(\lambda) = -\frac{3}{4}, \quad c_2(\lambda) = 6.$$

Comme le discriminant de P ne dépend que de c_2, on sait que $c_2(\lambda)$ ne prend pas les valeurs $-3/4$ ou 6 si λ n'est pas dans $\{-1, 1/2, 2, e^{\pm i\pi/3}\}$ (sinon, P aurait une racine multiple pour une autre valeur de λ).

Revenons aux indéterminées. La définition suivante de j est à présent presque motivée :

$$j = 6 - c_2.$$

Par construction, j est une fraction rationnelle en λ. Le dénominateur de j est $\lambda^2(\lambda-1)^2$. D'après ce que l'on a vu de l'annulation de $c_2(\lambda) - 6$, les zéros de j sont les valeurs $e^{\pm i\pi/3}$; comme j est une fraction à coefficients rationnels, son numérateur est donc une puissance de $\lambda^2-\lambda+1$, le polynôme minimal de $e^{\pm i\pi/3}$. De plus, le numérateur est de degré 6 et son coefficient dominant est 1. On peut donc affirmer (et contrôler par un calcul direct) :

$$j = \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

La définition de j permet d'écrire P de la façon suivante, ce qui conclut la preuve :

$$P(X) = X^6 - 3X^5 + (6-j)X^4 + (2j-7)X^3 + (6-j)X^2 - 3X + 1. \quad \square$$

1.6. Remarque. On le sait déjà, mais l'on peut vérifier à la main que j est invariant par le groupe de Galois de $\mathbb{K}(\lambda)/\mathbb{K}$ (il suffit de le faire pour $\lambda \mapsto -1/\lambda$ et $\lambda \mapsto 1-\lambda$, qui engendrent $\mathfrak{S}_3$). En d'autres termes, j est une fraction en les polynômes symétriques élémentaires σ_i. On trouve dans les

livres l'expression de j. On a :

$$j = \frac{(12\sigma_4 + \sigma_2^2 - 3\sigma_1\sigma_3)^3}{\Delta}, \quad \Delta = \Big(\prod_{1\leqslant i<j\leqslant 4}(z_i - z_j)\Big)^2,$$

où Δ désigne le discriminant de $\prod_{i=1}^4(X - z_i)$, c'est-à-dire le carré du déterminant de Vandermonde. (On peut faire trouver ou vérifier directement cette relation avec un logiciel de calcul formel. Par ailleurs, l'expression de Δ en fonction des σ_k est très compliquée.)

1.7. Remarque. Le théorème de Lüroth exprime que toute extension de $\mathbb{C}$ de degré de transcendance 1 est isomorphe à $\mathbb{C}(t)$, où t est une indéterminée. D'après ce théorème, on sait *a priori* que $\mathbb{C}(\lambda)^{\mathfrak{S}_4}$ est isomorphe à $\mathbb{C}(j)$ pour un $j \in \mathbb{C}(\lambda)$ convenable : ici, on économise l'application de ce théorème difficile et l'on gagne une expression explicite d'un générateur. On récupère tout de même un théorème d'unicité : un tel élément j qui engendre $\mathbb{C}(\lambda)^{\mathfrak{S}_4}$ est unique modulo $\mathrm{Aut}\big(\mathbb{C}(j)\big) \simeq \mathrm{Aut}\big(\mathbb{C}(t)\big)$, c'est-à-dire que j est unique modulo homographie, *i.e.* unique à substitution par $g\cdot j = (aj+b)/(cj+d)$ pour $g \in \mathrm{PGL}_2(\mathbb{C})$ près.

1.8. Remarque. La fraction rationnelle j apparaît dans la théorie des courbes elliptiques et des formes modulaires sous le nom d'*invariant modulaire*. Une *courbe elliptique* complexe est un groupe de la forme $E = \mathbb{C}/\Lambda$, où Λ est un réseau[2] de $\mathbb{C}$. Tout élément de Λ est une période de la fonction de Weierstrass $\wp$ associée au réseau et $\wp$ est solution d'une équation différentielle : $(\wp')^2 = 4\wp^2 - g_2\wp - g_3$, où $g_2 = g_2(\Lambda)$ et $g_3 = g_3(\Lambda)$ sont des « séries d'Eisenstein ». De plus, l'application $\mathbb{C} \to \mathbb{P}^2(\mathbb{C})$, $t \mapsto [\wp(t) : \wp'(t) : 1]$ se prolonge en une bijection de la courbe elliptique vers la variété projective de $\mathbb{P}^2(\mathbb{C})$ d'équation $Y^2Z = 4X^3 - g_2XZ^2 + g_3Z^3$. (Voir par exemple [5, proposition VI-2.5].)

Or, si l'on change de réseau, la classe d'isomorphisme de E (comme variété algébrique) ne dépend que du birapport $\lambda = [\infty, z_1, z_2, z_3]$, lorsque l'on écrit $4X^3 - g_2X - g_3 = 4(X - z_1)(X - z_2)(X - z_3)$. L'invariant modulaire j est une fonction[3] du réseau Λ via g_2 et g_3 ou, en changeant de paramètre, de λ :

$$j = \frac{27}{4}\frac{g_2^3}{\Delta} = \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}, \quad \text{où } \Delta = g_2^3 - 27g_3^2.$$

L'intérêt de l'invariant j est le suivant : deux courbes associées à λ et λ' sont isomorphes si et seulement si les images de λ et λ' par j sont égales.

[2] C'est-à-dire un sous-groupe discret qui engendre $\mathbb{C}$ comme espace vectoriel réel, et donc isomorphe à $\mathbb{Z}^2$.

[3] Tant de grandes responsabilités pour une si petite fonction !

Voir, sur les courbes elliptiques, l'excellent, mais quelque peu elliptique, [55, §1.11-1.12] et le légendaire [75, chapitre VII].

Interprétation géométrique de j (version 1)

Ce paragraphe est adapté de [55, §4.6]. Si l'on oublie tout ce qui concerne les quadruplets de points, on reste avec une action de $\mathfrak{S}_3$ sur $\mathbb{P}^1(\mathbb{C})$ via les six homographies

$$\lambda \mapsto \lambda,\ \lambda \mapsto \frac{\lambda-1}{\lambda},\ \lambda \mapsto \frac{-1}{\lambda-1},\ \lambda \mapsto \frac{1}{\lambda},\ \lambda \mapsto -\lambda+1,\ \lambda \mapsto \frac{\lambda}{\lambda-1},$$

et une application

$$j : \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C}), \quad \lambda \longmapsto \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

Par abus, λ, qui était une indéterminée, est désormais une variable générique dans $\mathbb{P}^1(\mathbb{C})$. La proposition suivante exprime que j permet d'identifier l'ensemble-quotient $\mathbb{P}^1/\mathfrak{S}_3$ avec $\mathbb{P}^1$.

1.9. Proposition.

(i) *L'application j est surjective. Soient $\lambda, \lambda' \in \mathbb{P}^1(\mathbb{C})$. Alors : $j(\lambda) = j(\lambda')$ si et seulement si λ et λ' sont dans la même orbite sous $\mathfrak{S}_3$.*

(ii) *Chacune des six régions délimitées par les traits gras de la figure 1.1 est un domaine fondamental de l'action de $\mathfrak{S}_3$.*

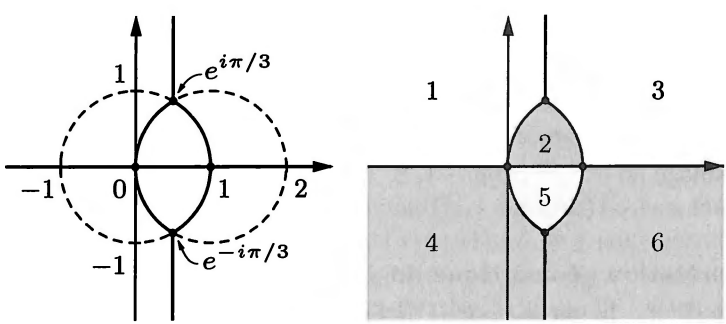


Figure 1.1. *Domaine fondamental pour l'action de $\mathfrak{S}_3$ sur $\mathbb{P}^1$*

Ici, « domaine fondamental » signifie que toute orbite rencontre l'adhérence de chaque région en un point et, si l'intersection se situe à l'intérieur, alors elle ne contient qu'un seul point.

Démonstration. (i) Soit $j_0 \in \mathbb{P}^1(\mathbb{C})$. Si j_0 est différent de ∞, ses antécédents par j sont les racines du polynôme P introduit au paragraphe précédent :

$$P = X^6 - 3X^5 + (6 - j_0)X^4 + (2j_0 - 7)X^3 + (6 - j_0)X^2 - 3X + 1.$$

Par construction de P, si l'une des racines est λ, l'ensemble des racines de P forme l'orbite de λ sous l'action de $\mathfrak{S}_3$. D'autre part, si j_0 est ∞, ses antécédents sont les pôles de j et le point ∞.

(ii) Les régions décrites par la figure 1.1 sont délimitées par les cercles $\mathscr{C}_0$ et $\mathscr{C}_1$ de centres respectifs 0 et 1 et de rayon 1, par l'axe réel et par la droite d'équation $\mathrm{Re}(\lambda) = 1/2$. On les numérote de 1 à 6. L'homographie $\lambda \mapsto 1 - \lambda$ est la symétrie de centre $1/2$: elle échange les régions 1 et 6 ; 2 et 5 ; 3 et 4. L'homographie $\lambda \mapsto 1/\lambda$ stabilise le cercle-unité et en permute l'intérieur et l'extérieur ; elle échange le cercle $\mathscr{C}_1$ et la droite d'équation $\mathrm{Re}(\lambda) = 1/2$, l'intérieur du disque et le demi-plan $\mathrm{Re}(\lambda) > 1/2$; elle fixe l'axe réel et permute les deux demi-plans qu'il délimite. Par suite, elle permute les régions 2 et 6, les régions 4 et 3 et les régions 1 et 5. On termine en utilisant le fait que $\lambda \mapsto 1/\lambda$ et $\lambda \mapsto 1 - \lambda$ engendrent $\mathfrak{S}_3$. □

1.10. Remarque. Plutôt que numéroter les régions par un nombre arbitraire entre 1 et 6, on peut suivre le destin d'un élément λ appartenant (par exemple) à la région 2 sous le groupe et numéroter les régions par l'homographie associée à un élément de $\mathfrak{S}_3$.

1.11. Remarque. On dit que j est un *revêtement ramifié* d'ordre 6. Cela signifie en gros qu'un élément générique w de $\mathbb{P}^1(\mathbb{C})$ a six antécédents distincts par j, sauf ∞ (qui a trois antécédents, ∞, 0 et 1, chacun de multiplicité 2, en un sens évident), 0 (qui a deux antécédents $e^{\pm i\pi/3}$, de multiplicité 3) et $27/4$ (qui a trois antécédents -1, 2 et $1/2$, de multiplicité 2). Plus précisément, un w générique est le centre d'un disque D tel que $j^{-1}(D)$ est la réunion de six disques D'_k sur lesquels $j|_{D'_k} : D'_k \to D$ est biholomorphe ; au voisinage de $e^{\pm i\pi/3}$ (resp. -1, 2, $1/2$), j est biholomorphiquement équivalente à $z \mapsto z^3$ (resp. $z \mapsto z^2$) au voisinage de 0.

Interprétation géométrique de j (version 2)

Notons $(\mathbb{P}^1)^4_{\mathrm{reg}}$ la partie de $\mathbb{P}^1(\mathbb{C})^4$ formée des quadruplets ordonnés d'éléments deux à deux distincts de $\mathbb{P}^1(\mathbb{C})$. Les groupes $\mathrm{PGL}_2(\mathbb{C})$ et $\mathfrak{S}_4$ agissent naturellement sur $(\mathbb{P}^1)^4_{\mathrm{reg}}$ et les actions commutent : pour $g \in \mathrm{PGL}_2(\mathbb{C})$, $\pi \in \mathfrak{S}_4$ et $(z_1, z_2, z_3, z_4) \in (\mathbb{P}^1)^4_{\mathrm{reg}}$, on pose :

$$g \cdot (z_1, z_2, z_3, z_4) = (g \cdot z_1, g \cdot z_2, g \cdot z_3, g \cdot z_4),$$
$$\pi \cdot (z_1, z_2, z_3, z_4) = (z_{\pi^{-1}(1)}, z_{\pi^{-1}(2)}, z_{\pi^{-1}(3)}, z_{\pi^{-1}(4)}).$$

Par [H2G2, proposition X-1.2.13], le birapport est invariant par homographies et même, il est un invariant complet pour les orbites de quadruplets ordonnés sous le groupe $G = \mathrm{PGL}_2(\mathbb{C})$:

$$\begin{array}{rcl} \lambda : (\mathbb{P}^1)^4_{\mathrm{reg}}/\,\mathrm{PGL}_2(\mathbb{C}) & \longrightarrow & \mathbb{P}^1(\mathbb{C}) \setminus \{0,1,\infty\} \\ G\cdot(z_1,z_2,z_3,z_4) & \longmapsto & [z_1,z_2,z_3,z_4]. \end{array}$$

De façon analogue, on va interpréter j comme un invariant pour les quadruplets non ordonnés. On peut identifier l'orbite d'un quadruplet (z_1,z_2,z_3,z_4) sous $\mathfrak{S}_4$ à l'ensemble $\{z_1,z_2,z_3,z_4\}$ et on fait agir naturellement $G = \mathrm{PGL}_2(\mathbb{C})$ sur ces ensembles.

1.12. Proposition. *Étant donné un quadruplet ordonné* $(z_1,z_2,z_3,z_4) \in (\mathbb{P}^1)^4_{\mathrm{reg}}$, *le nombre complexe* $j\big([z_1,z_2,z_3,z_4]\big)$ *ne dépend que de l'ensemble* $\{z_1,z_2,z_3,z_4\}$. *On note ce complexe :* $J\big(\{z_1,z_2,z_3,z_4\}\big)$.

De plus, l'application J *établit une bijection entre orbites de quadruplets non ordonnés sous l'action de* $\mathrm{PGL}_2(\mathbb{C})$ *et points de* $\mathbb{P}^1(\mathbb{C}) \setminus \{\infty\}$.

On résume la proposition dans un diagramme commutatif :

$$\begin{array}{ccccccc} (\mathbb{P}^1)^4_{\mathrm{reg}} & \twoheadrightarrow & (\mathbb{P}^1)^4_{\mathrm{reg}}/\,\mathrm{PGL}_2 & \xrightarrow{\lambda} & \mathbb{P}^1 \setminus \{0,1,\infty\} & \hookrightarrow & \mathbb{P}^1 \\ \downarrow & & \downarrow & & \downarrow j & & \downarrow j \\ \mathfrak{S}_4\backslash(\mathbb{P}^1)^4_{\mathrm{reg}} & \twoheadrightarrow & \mathfrak{S}_4\backslash(\mathbb{P}^1)^4_{\mathrm{reg}}/.\mathrm{PGL}_2 & \xrightarrow{J} & \mathbb{P}^1 \setminus \{\infty\} & \hookrightarrow & \mathbb{P}^1, \end{array}$$

où les applications du carré central sont :

$$\begin{array}{ccc} (z_1,z_2,z_3,z_4) & \xmapsto{\lambda} & [z_1,z_2,z_3,z_4] \\ \downarrow & & \downarrow j \\ \{z_1,z_2,z_3,z_4\} & \xmapsto{J} & j\big([z_1,z_2,z_3,z_4]\big). \end{array}$$

Démonstration. Presque tout a déjà été dit. Le fait que $j\big([z_1,z_2,z_3,z_4]\big)$ ne dépend pas de l'ordre des z_i résulte de l'invariance de j par permutations. Par définition de j ou par la proposition 1.9, la fibre de j au dessus de ∞ est $\{\infty,0,1\}$, et j établit une surjection de $\mathbb{P}^1 \setminus \{\infty,0,1\}$ sur $\mathbb{P}^1 \setminus \{\infty\}$. Comme l'application λ est aussi surjective ($z_4 = [\infty,0,1,z_4]$ pour tout z_4) J l'est encore.

Vérifions l'injectivité. Supposons que $\{z_1,\ldots,z_4\}$ et $\{z'_1,\ldots,z'_4\}$ aient la même image par J. Par la proposition 1.9, $[z_1,\ldots,z_4]$ et $[z'_1,\ldots,z'_4]$ sont dans la même $\mathfrak{S}_3$-orbite. Vu que l'action de $\mathfrak{S}_4$ sur les variables du birapport se factorise à travers $\mathfrak{S}_3$ (proposition 1.3), il existe une permutation

$\sigma \in \mathfrak{S}_4$ telle que

$$[z_{\sigma(1)}, z_{\sigma(2)}, z_{\sigma(3)}, z_{\sigma(4)}] = [z'_1, z'_2, z'_3, z'_4].$$

Mais alors, par [H2G2, proposition X-1.2.13], le birapport classe les quadruplets de points distincts et il existe donc une homographie qui envoie $(z_{\sigma 1}, z_{\sigma 2}, z_{\sigma 3}, z_{\sigma 4})$ sur (z'_1, z'_2, z'_3, z'_4), de sorte que les ensembles $\{z_1, \dots, z_4\}$ et $\{z'_1, \dots, z'_4\}$ sont dans la même $\big(\mathfrak{S}_4 \times \mathrm{PGL}_2(\mathbb{C})\big)$-orbite. □

1.13. Remarque. On peut ainsi considérer $\mathbb{P}^1(\mathbb{C})$ comme compactification naturelle de $(\mathbb{P}^1)^4_{\mathrm{reg}}/\mathrm{PGL}_2(\mathbb{C})$ (grâce à λ) et aussi de $\mathfrak{S}_4\backslash(\mathbb{P}^1)^4_{\mathrm{reg}}/\mathrm{PGL}_2(\mathbb{C})$ (grâce à J). Notons que l'on a déjà vu la première compactification dans [H2G2, proposition X-1.2.16].

2. Plan hyperbolique

Чёрт: Мне случалось делать вещи и потруднее, дорогой профессор.
Семен Райтбурт, "Математик и чёрт", 1972[4].

Nous avons déjà rencontré un avatar du plan hyperbolique dans [H2G2, exercices II-6.18, II-6.22 et X-3.16], le demi-plan de Poincaré

$$\mathscr{H} = \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}.$$

Nous allons mettre sur $\mathscr{H}$ une distance intéressante car elle possède un gros groupe d'isométries, $\mathrm{PSL}_2(\mathbb{R})$: la géométrie dite hyperbolique, que l'on peut alors développer, est très riche. Nous ne nous y aventurons pas vraiment —voir l'immense [66]. À la place, nous allons la réaliser dans plusieurs espaces isométriques à $\mathscr{H}$. Le point le plus intéressant est le passage d'un modèle qui relève de la géométrie complexe (sous l'avatar précédent $\mathscr{H}$) à un modèle de géométrie réelle; le pont entre les deux consiste à regarder le cône isotrope d'un produit scalaire euclidien... Selon la réalisation, $\mathrm{PSL}_2(\mathbb{R})$ apparaît comme sous-groupe de $\mathrm{PSL}_2(\mathbb{C})$ ou de $\mathrm{PGL}_3(\mathbb{R})$. C'est une notion de birapport adaptée à chaque version qui fait le lien entre elles.

2.1. Droite projective réelle, demi-plan de Poincaré et leurs stabilisateurs

La droite projective réelle $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$ est un fermé de la droite projective complexe $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. Son complémentaire est la réunion de deux composantes connexes, images l'une de l'autre par la conjugaison complexe, dont l'une est le demi-plan de Poincaré.

[4] *Le diable : « J'ai déjà fait des choses plus difficiles, cher professeur ».* Simon Raytburt, *The Mathematician and the Devil*, 1972.

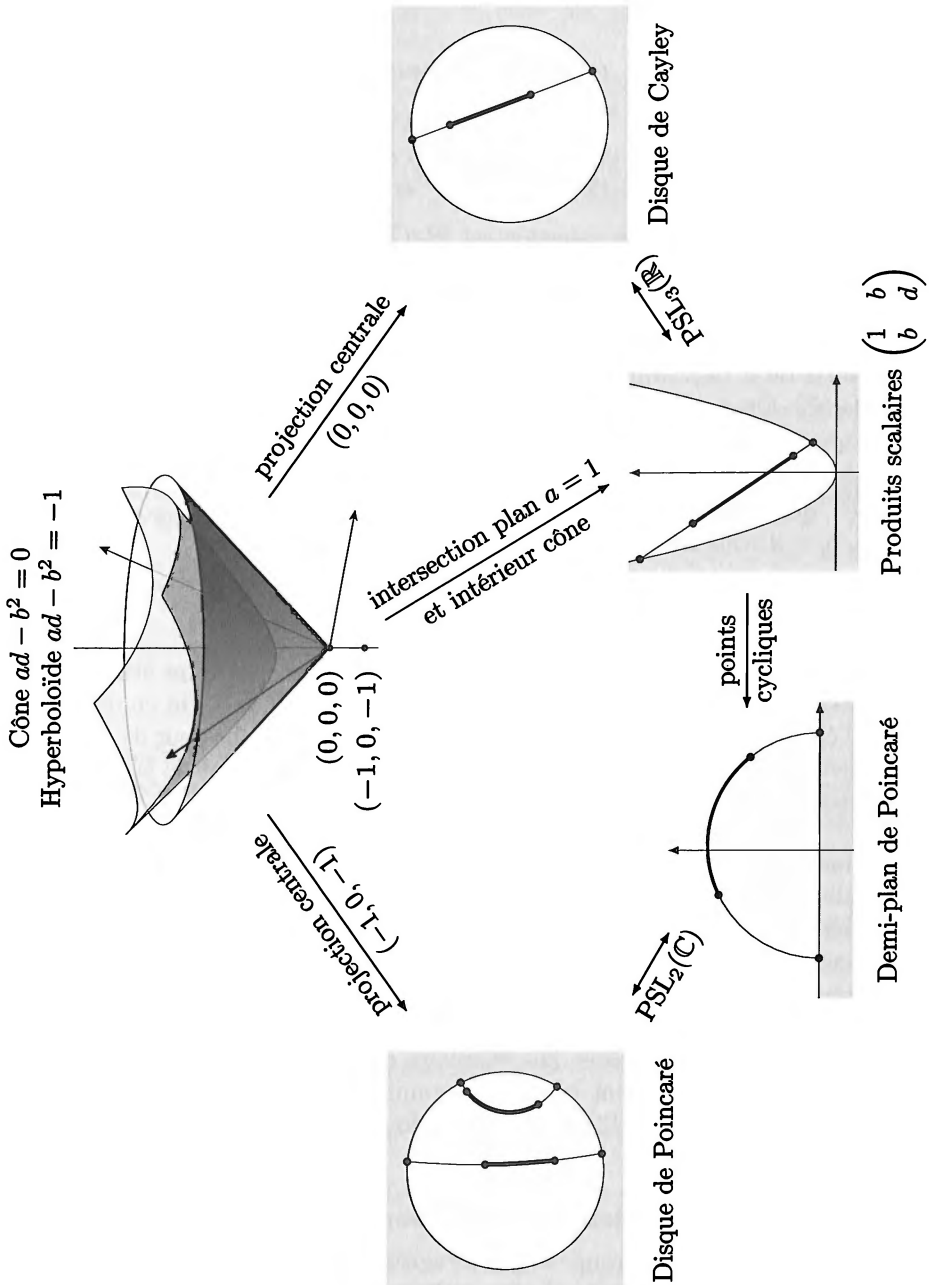


Figure 2.1. *Cinq modèles du plan hyperbolique*

2.2. Lemme

(i) *On a :*
$$\mathrm{PGL}_2(\mathbb{C}) = \mathrm{PSL}_2(\mathbb{C}) \quad \textit{et} \quad [\mathrm{PGL}_2(\mathbb{R}) : \mathrm{PSL}_2(\mathbb{R})] = 2.$$

(ii) *Le stabilisateur de* $\mathbb{P}^1(\mathbb{R})$ *dans* $\mathrm{PGL}_2(\mathbb{C})$ *est* $\mathrm{PGL}_2(\mathbb{R})$.

(iii) *Le stabilisateur de* $\mathscr{H}$ *dans* $\mathrm{PGL}_2(\mathbb{C})$ *est* $\mathrm{PSL}_2(\mathbb{R})$ *; une homographie de* $\mathrm{PGL}_2(\mathbb{R}) \setminus \mathrm{PSL}_2(\mathbb{R})$ *permute* $\mathscr{H}$ *et*[5] $\overline{\mathscr{H}}$.

Démonstration. (i) Cette assertion est [H2G2, lemme X-2.2].

(ii) Soit h une homographie complexe qui stabilise $\mathbb{P}^1(\mathbb{R})$. Par [H2G2, proposition X-1.2.7], il existe une unique homographie $h' \in \mathrm{PGL}_2(\mathbb{R})$ qui envoie ∞, 0, 1 respectivement sur $h(\infty)$, $h(0)$ et $h(1)$, qui sont trois éléments distincts de $\mathbb{P}^1(\mathbb{R})$. Mais une telle homographie est également unique dans $\mathrm{PGL}_2(\mathbb{C})$. On a donc : $h = h'$ ou, en d'autres termes : $h \in \mathrm{PGL}_2(\mathbb{R})$.

(iii) Comme l'action de $\mathrm{PGL}_2(\mathbb{C})$ est continue, si une homographie stabilise $\mathscr{H}$, elle stabilise également son bord, vu dans l'espace topologique $\mathbb{P}^1(\mathbb{C})$, qui est $\mathbb{P}^1(\mathbb{R})$: elle appartient donc à $\mathrm{PGL}_2(\mathbb{R})$. De plus, pour $z \in \mathbb{C}$ et a, b, c, d réels tels que $ad - bc \neq 0$, on a :
$$\mathrm{Im}\,\frac{az+b}{cz+d} = \frac{ad-bc}{|cz+d|^2}\,\mathrm{Im}\,z.$$

Grâce à l'assertion (i), ou sans, on voit que la classe $[g]$ d'un élément g de $\mathrm{GL}_2(\mathbb{R})$ est dans $\mathrm{PSL}_2(\mathbb{R})$ si et seulement si $\det(g) > 0$. On en déduit, par l'égalité des parties imaginaires ci-dessus, que le stabilisateur de $\mathscr{H}$ est contenu dans $\mathrm{PSL}_2(\mathbb{R})$. L'inclusion inverse résulte également de la formule ci-dessus. □

On munit $\mathbb{C} = \mathbb{R}^2$ de sa structure d'espace euclidien canonique. L'orthogonalité des cercles et droites sera prolongée à $\mathbb{P}^1(\mathbb{C})$: deux cercles ou droites sont orthogonaux dans $\mathbb{P}^1(\mathbb{C})$ si leur intersection avec $\mathbb{R}^2$ le sont. Les cercles de $\mathbb{P}^1(\mathbb{C})$ dont le centre est réel sont orthogonaux à $\mathbb{P}^1(\mathbb{R})$: une telle propriété est préservée par homographies, si bien que ces cercles sont globalement stables par $\mathrm{PSL}_2(\mathbb{R})$. Ils forment la réunion des faisceaux[6] dont les *points limites* sont réels. Les faisceaux orthogonaux sont les faisceaux dont les *points bases* sont complexes conjugués, qui forment une famille de cercles stabilisés par $\mathrm{PSL}_2(\mathbb{R})$. On va donner une interprétation géométrique de ces familles.

2.3. Distance sur le demi-plan de Poincaré

On vient de voir que le groupe $\mathrm{PSL}_2(\mathbb{R})$ agit sur $\mathscr{H}$ par homographies. Dans ce paragraphe, on fait du demi-plan de Poincaré $\mathscr{H}$ un espace métrique de

[5] Ici, on désigne par $\overline{\mathscr{H}}$ l'image de $\mathscr{H}$ par la conjugaison complexe.

[6] La notion classique de faisceau de cercles est illustrée dans l'annexe VI-A.

sorte que cette action de $\mathrm{PSL}_2(\mathbb{R})$ se fasse par isométries. Pour cela, on munit $\mathscr{H}$ de la métrique suivante :

$$\mathrm{d}s^2 = \frac{\mathrm{d}x^2 + \mathrm{d}y^2}{y^2} = -4\,\frac{\mathrm{d}z\,\mathrm{d}\overline{z}}{(z-\overline{z})^2}.$$

Sens. Si $\gamma : [0,1] \to \mathscr{H}$, $t \mapsto \big(x(t), y(t)\big)$ est une courbe de classe $\mathscr{C}^1$, sa longueur est, par définition :

$$\ell(\gamma) = \int_\gamma \mathrm{d}s = \int_0^1 \frac{\sqrt{\dot{x}(t)^2 + \dot{y}(t)^2}}{y(t)}\,\mathrm{d}t,$$

où $\dot{x}$ et $\dot{y}$ sont les dérivées de x et y (« par rapport à t »).

2.4. Proposition. *La métrique* $\mathrm{d}s^2 = (\mathrm{d}x^2 + \mathrm{d}y^2)/y^2$ *est invariante par homographies : pour* $g \in \mathrm{PSL}_2(\mathbb{R})$ *et* $\gamma : [0,1] \to \mathscr{H}$, *on a :* $\ell(g\cdot\gamma) = \ell(\gamma)$.

Démonstration. Supposons que $g \cdot z = z + u$ pour $u \in \mathbb{R}$ fixé, on a bien : $\ell(g\cdot\gamma) = \ell(\gamma)$.

Supposons que $g \cdot z = -1/z$. Alors, avec $z' = -1/z$, on a : $\mathrm{d}z' = -z^{-2}\mathrm{d}z$, d'où :

$$\mathrm{d}s'^2 = -4\frac{\mathrm{d}z'\,\mathrm{d}\overline{z}'}{(z'-\overline{z}')^2} = -4\frac{\frac{\mathrm{d}z}{z^2}\,\frac{\mathrm{d}\overline{z}}{\overline{z}^2}}{\big(\frac{1}{z}-\frac{1}{\overline{z}}\big)^2} = -4\frac{\mathrm{d}z\,\mathrm{d}\overline{z}}{(z-\overline{z})^2} = \mathrm{d}s^2.$$

Il en résulte que $\ell(g\cdot\gamma) = \ell(\gamma)$ pour $g \cdot z = -1/z$. On peut aussi faire un changement de variable adéquat dans l'intégrale en travaillant en coordonnées (x, y), mais c'est moins efficace. Pour conclure, on utilise le lemme suivant. □

2.5. Lemme. *Les classes de* $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ *et* $T_u = \left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right)$ *($u \in \mathbb{R}$) engendrent le groupe* $\mathrm{PSL}_2(\mathbb{R})$.

Démonstration. D'abord, on vérifie que ST_uS^{-1} est la transposée de T_{-u}, donc S et les T_u engendrent toutes les transvections, donc ils engendrent tout le groupe, d'après [H2G2, exercice IV-B.1]. □

On définit à présent une distance et ses géodésiques.

2.6. Définition. On appelle *distance hyperbolique* entre deux points m et n de $\mathscr{H}$ le nombre :

$$D_{\mathscr{H}}(m,n) = \inf_\gamma \ell(\gamma),$$

où $\gamma : [0,1] \to \mathscr{H}$ parcourt l'ensemble des courbes $\mathscr{C}^1$ telles que $\gamma(0) = m$ et $\gamma(1) = n$. S'il existe une courbe dont la longueur est égale à la borne inférieure, on l'appelle *géodésique* reliant m et n.

Problèmes : est-ce qu'une telle courbe existe ? est-ce qu'elle est unique ? Eh bien, oui ! Et ce n'est pas vraiment étonnant d'y voir apparaître le birapport, puisque la distance est invariante pour les homographies de $\mathrm{PSL}_2(\mathbb{R})$.

2.7. Proposition. *Soient $m, n \in \mathscr{H}$, $m \neq n$. Il existe un unique cercle contenant m et n et orthogonal à l'axe réel $\{\mathrm{Im} = 0\}$. L'arc de ce cercle délimité par m et n qui est contenu dans $\mathscr{H}$ est l'unique géodésique reliant m et n. De plus, si m_0 et n_0 sont les points d'intersection du cercle avec l'axe réel, de sorte à trouver dans l'ordre m_0, m, n et n_0, on a :*

$$D_{\mathscr{H}}(m,n) = \ln [m, n, n_0, m_0].$$

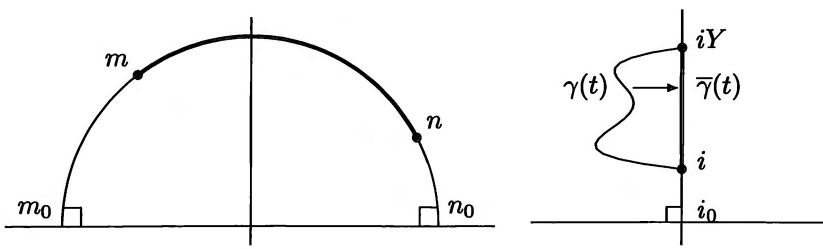


Figure 2.2. *Géodésiques du demi-plan de Poincaré*

Idée-clé. On régularise la figure ! Dans l'esprit de [H2G2, chapitre IX], on se ramène via une action de groupes à un cas simple. Dans le cas particulier de la figure de droite, il est très facile de voir que la géodésique est le segment $[i, iY]$ et que la longueur de ce segment est $\ln(Y)$. On exprime cette quantité de sorte à la rendre invariante par les isométries de $\mathscr{H}$ et l'on ramène le cas général à ce cas particulier par l'action de $\mathrm{PSL}_2(\mathbb{R})$.

Démonstration. La première assertion est élémentaire : si m et n n'ont pas la même partie réelle, le cercle cherché est le cercle circonscrit au triangle dont les sommets sont m, n et $\overline{n}$; son centre est sur la médiatrice du segment $[n\overline{n}]$ qui est l'axe réel, donc le cercle contient automatiquement $\overline{m}$; si m et n ont la même partie réelle, ce cercle est la droite verticale qui les contient. Soient m_0 et n_0 les intersections de ce cercle avec l'axe réel (si $\mathrm{Re}(m) = \mathrm{Re}(n)$, l'un de ces points est ∞).

Cas particulier. On suppose que l'on a : $m = i$, $n = iY$ (où $i^2 = -1$ et Y est un réel strictement supérieur à 1). Fixons une courbe $\gamma : [0,1] \to \mathscr{H}$ de classe $\mathscr{C}^1$, avec $\gamma(0) = i$ et $\gamma(1) = iY$. Soit $\overline{\gamma} : [0,1] \to \mathscr{H}$ la projection orthogonale de γ sur l'axe des ordonnées : si $\gamma(t) = x(t) + iy(t)$, alors

$\overline{\gamma}(t) = iy(t)$. On a :

$$\ell(\gamma) = \int_0^1 \frac{\sqrt{\dot{x}(t)^2 + \dot{y}(t)^2}}{y(t)} \mathrm{d}t \geqslant \int_0^1 \frac{\sqrt{\dot{y}(t)^2}}{y(t)} \mathrm{d}t = \int_0^1 \frac{|\dot{y}(t)|}{y(t)} \mathrm{d}t = \ell(\overline{\gamma}).$$

On voit ainsi qu'une courbe est plus longue que sa projection sur l'axe imaginaire pur, et l'on en déduit que la courbe la plus courte qui relie i et iY est le segment $[i, iY]$. Ainsi, ce segment est l'unique géodésique entre i et iY. De plus, en paramétrant ce segment par $\gamma(t) = i\big(1 + t(Y-1)\big)$, où t décrit $[0,1]$, on obtient :

$$D_{\mathscr{H}}(i, iY) = \int_0^1 \frac{Y-1}{1+t(Y-1)} \mathrm{d}t = \int_1^Y \frac{\mathrm{d}y}{y} = \ln Y = \ln [i, iY, \infty, 0].$$

Pour $m = i$ et $n = iY$, on a : $m_0 = 0$ et $n_0 = \infty$, et l'on a démontré la formule dans ce cas.

Cas général. Vérifions qu'il existe une homographie $g \in \mathrm{PSL}_2(\mathbb{R})$ qui envoie m sur i et qui envoie n sur un point de partie réelle nulle iY, avec Y réel, $Y > 1$. En effet, si m et n n'ont pas la même partie réelle, on applique successivement : une homographie $h_1 \in \mathrm{PSL}_2(\mathbb{R})$ qui envoie m_0 sur 0 et n_0 sur ∞ (ainsi, $\mathrm{Re}\, h_1(m) = \mathrm{Re}\, h_1(n) = 0$ —pourquoi ?) ; une homothétie réelle h_2 pour envoyer $h_1(m)$ sur i ; alors, $g = h_2 h_1$ envoie m sur i et n sur iY ($Y \in \mathbb{R}^{+*}$) ; si $Y < 1$, on remplace $h_2 h_1$ par $h_3 h_2 h_1$, où $h_3 : z \mapsto -1/z$. Et si m et n ont la même partie réelle, on procède de même avec une translation pour h_1.

Comme les homographies sont des isométries de $\mathscr{H}$, on a : $D_{\mathscr{H}}(m,n) = D_{\mathscr{H}}(i, iY)$ et, par construction : $g(m_0) = 0$, $g(n_0) = \infty$. Il en résulte que la géodésique reliant m et n est l'image réciproque par g du segment $[i, iY]$. De plus, par invariance du birapport, on a :

$$D_{\mathscr{H}}(m,n) = D_{\mathscr{H}}(i, iY) = \ln [i, iY, \infty, 0] = \ln [m, n, n_0, m_0]. \qquad \square$$

2.8. Remarque. La formule qui exprime $D_{\mathscr{H}}(m,n)$ est spectaculairement semblable à la *distance de Hilbert*, voir [H2G2, §X-2.3]. On en verra deux explications au paragraphe 2.16.

2.9. Remarque. Les géodésiques passant par un point à l'infini fixé de $\mathscr{H}$, c'est-à-dire les géodésiques dont l'adhérence contient un point $m_0 \in \mathbb{P}^1(\mathbb{R})$, forment un faisceau de cercles[7] tangents. On verra ci-dessous une interprétation du faisceau tangent qui lui est orthogonal.

[7] Les pages qui suivent utilisent la notion de faisceau assez intensément. Pour une approche élémentaire, on pourra consulter [4], §III-4. Pour une version plus algébrique, voir le paragraphe VI-3 ci-dessus et l'annexe VI-A.

Cercles hyperboliques

2.10. Définition. Étant donnés deux points m et n de $\mathscr{H}$, on appelle *cercle hyperbolique* centré en m et passant par n l'ensemble des points de $\mathscr{H}$ qui sont à la même distance hyperbolique de m que n, c'est-à-dire :

$$\{n' \in \mathscr{H},\ D_{\mathscr{H}}(m,n) = D_{\mathscr{H}}(m,n')\}.$$

Question. Comment décrire ces cercles hyperboliques ?

2.11. Cercles hyperboliques, version géométrique

Pour des raisons qui relèvent de la géométrie différentielle amusante, les cercles sont les *trajectoires orthogonales des géodésiques* — voir l'annexe A. En d'autres termes, un cercle de centre m est une courbe dont la tangente en tout point n est orthogonale à la géodésique reliant m et n.

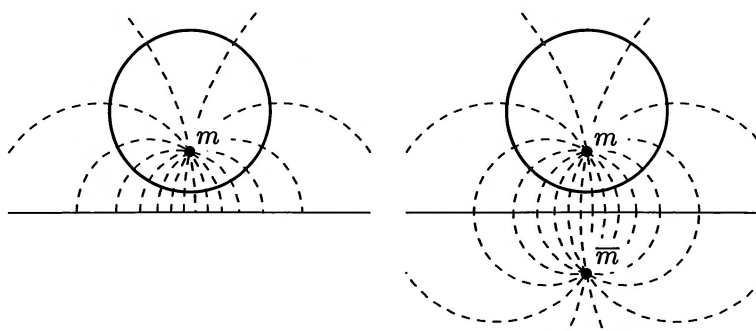


Figure 2.3. *Géodésiques issues de m, et cercle hyperbolique*

Or, toutes les géodésiques sont situées sur des cercles orthogonaux à l'axe réel, donc symétriques par rapport à celui-ci. Les géodésiques contenant m contiennent donc son conjugué $\overline{m}$. On voit ainsi que les géodésiques forment le *faisceau de cercles à points bases* m et $\overline{m}$ (du moins, la partie qui est contenue dans $\mathscr{H}$). Les trajectoires orthogonales de ces cercles forment le *faisceau de cercles à points limites* m et $\overline{m}$. Ainsi, un cercle hyperbolique est un cercle euclidien.

2.12. Remarque (Daniel Perrin, [66]). Un cercle du plan euclidien n'est autre qu'une orbite sous le stabilisateur du centre du cercle. L'intérêt de ce point de vue, c'est d'étendre la notion de cercle à une gigantesque variété de situations. En effet, chaque fois qu'un groupe G agit sur un ensemble X, on peut définir le « cercle » centré en un point x de X qui passe par un autre point y de X comme l'orbite $G_x \cdot y$ de y sous le stabilisateur de x.

2.13. Cercles hyperboliques, version groupes

Soit m un point de $\mathscr{H}$. L'homographie $h : z \mapsto (z-m)/(z-\overline{m})$ transforme le faisceau de cercles à points limites m et $\overline{m}$ en le faisceau des cercles à points limites 0 et ∞, qui sont les cercles centrés en l'origine. Dans ce faisceau, l'axe réel $\mathbb{P}^1(\mathbb{R})$, qui est la médiatrice du segment d'extrémités m et $\overline{m}$, est envoyé sur le cercle-unité. Le stabilisateur de m dans $\mathrm{PSL}_2(\mathbb{R})$ est l'intersection des stabilisateurs de m et de $\mathbb{P}^1(\mathbb{R})$; un élément du stabilisateur fixe automatiquement $\overline{m}$. Il est conjugué par h en l'intersection des stabilisateurs de 0 et du cercle-unité dans $\mathrm{PGL}_2(\mathbb{C})$, c'est-à-dire le groupe $\mathrm{U}_1(\mathbb{C})$ des transformations $w \mapsto e^{i\theta}w$, où $\theta \in \mathbb{R}/2\pi\mathbb{Z}$. En effet, les homographies qui fixent $0 = h(m)$ et $\infty = h(\overline{m})$ sont les fonctions linéaires $z \mapsto az$, $a \in \mathbb{C}^*$; parmi elles, celles qui stabilisent le cercle-unité correspondent aux complexes a de module 1.

Les orbites sous le groupe $\mathrm{U}_1(\mathbb{C})$ sont les cercles centrés en l'origine : grâce à h^{-1}, on obtient ainsi que les orbites sous le stabilisateur de m sont exactement les cercles du faisceau à points limites m et $\overline{m}$.

Ainsi, comme dans le plan euclidien, la caractérisation des cercles par l'action du stabilisateur du centre s'identifie à la définition géométrique (ensemble de points équidistants) — ce n'est pas si étonnant car le groupe qui agit, $\mathrm{PSL}_2(\mathbb{R})$, est justement le groupe des isométries de $\mathscr{H}$.

2.14. Horocycles : cercles centrés à l'infini

Grisé par ce succès, on peut pousser à l'infini la construction précédente. Cela signifie que l'on prolonge naturellement l'action de $\mathrm{PSL}_2(\mathbb{R})$ au bord de $\mathscr{H}$ vu comme partie de $\mathbb{P}^1(\mathbb{C})$, c'est-à-dire à $\overline{\mathscr{H}} = \mathscr{H} \cup \mathbb{P}^1(\mathbb{R})$ (sur la sphère de Riemann, l'hémisphère qui correspond au demi-plan de Poincaré a pour bord l'équateur).

Définition. On appelle *horocycle* du demi-plan de Poincaré toute orbite du stabilisateur d'un point de $\mathbb{P}^1(\mathbb{R})$ pour l'action de $\mathrm{PSL}_2(\mathbb{R})$ sur $\mathscr{H}$.

Lorque $m = \infty$, on se convainc que le stabilisateur de m est le groupe des translations $z \mapsto z + b$, $b \in \mathbb{R}$. Les orbites de ce groupe sont les droites horizontales.

Lorsque $m = 0$, le stabilisateur de m est le groupe des homographies $z \mapsto z/(cz+1)$, $c \in \mathbb{R}$: en effet, si une homographie $z \mapsto (az+b)/(cz+d)$ fixe 0, alors $b = 0$, on peut donc supposer $a = 1$ et l'on a toujours $d = ad - bc = 1$. C'est bien le conjugué du stabilisateur de ∞ par l'application $h : z \mapsto -1/z$, qui envoie 0 sur ∞. Les orbites sont les images des droites horizontales par h, ce sont des cercles tangents à l'axe réel en 0 (on peut par exemple le vérifier directement ou invoquer la préservation du contact par l'homographie h).

Lorsque m est un réel, il n'y a qu'à transformer 0 en m par la translation $z \mapsto z+m$ et en déduire que les orbites sous le stabilisateur de p forment le faisceau tangent contenant m dont les tangentes sont orthogonales à l'axe réel.

Comme promis plus haut, on retrouve ainsi les faisceaux tangents en un point de l'axe réel dont la tangente est orthogonale à celui-ci, c'est-à-dire le faisceau orthogonal des géodésiques qui contiennent ce point, comme la famille des « cercles hyperboliques » centrés en ce point qui, pour $\mathscr{H}$, est à l'infini. Le terme consacré pour ces « cercles » centrés à l'horizon est *horocycle*.

2.15. Orbites des sous-groupes à un paramètre dans le demi-plan de Poincaré

On reprend les idées et notations du paragraphe VI-3.18. On fixe X non nul dans $\mathfrak{sl}_2(\mathbb{R})$ et l'on note $\varphi_X : \mathbb{R} \to \mathrm{PSL}_2(\mathbb{R})$, $t \mapsto \exp(tX)$. On a classé ces sous-groupes à un paramètre en trois types selon le spectre de X : hyperbolique, elliptique et parabolique. On réinterprète cette trichotomie en termes d'isométries de $\mathscr{H}$ — voir les figures de l'annexe VI-A.

▷ Un sous-groupe *de type parabolique* est conjugué dans $\mathrm{PSL}_2(\mathbb{R})$ à $z \mapsto z+t$ (avec $t \in \mathbb{R}$). Les orbites des groupes de ce type sont donc les horocycles du paragraphe 2.14, elles forment les faisceaux tangents dont le point base est réel et la tangente est l'axe réel $\mathbb{P}^1(\mathbb{R})$. Le point base de φ_X est d'ailleurs l'image dans $\mathbb{P}^1(\mathbb{R})$ d'un vecteur propre de X.

▷ Un sous-groupe *de type elliptique* est conjugué dans $\mathrm{PSL}_2(\mathbb{R})$ au stabilisateur $\mathrm{SO}_2(\mathbb{R})$ de i. Les orbites des groupes de ce type sont donc les cercles hyperboliques ; elles forment les faisceaux à points limites dont les points limites sont complexes conjugués. Les points limites du faisceau sont les images dans $\mathbb{P}^1(\mathbb{C})$ de vecteurs propres de $X \in \mathscr{M}_2(\mathbb{C})$.

▷ Un sous-groupe *de type hyperbolique* est conjugué à $z \mapsto e^{2t}z$ (avec $t \in \mathbb{R}$) dans $\mathrm{PSL}_2(\mathbb{R})$. Les orbites sont donc les cercles passant par les points fixes des homographies qui composent le groupe, qui proviennent des vecteurs propres de la matrice X de départ ; elles forment les faisceaux à points bases dont les points bases sont réels. Les points bases du faisceau sont les vecteurs propres de $X \in \mathscr{M}_2(\mathbb{R})$.

Ainsi, on observe une correspondance entre paires de faisceaux stables par conjugaison complexe et sous-groupes à un paramètre de $\mathrm{PSL}_2(\mathbb{R})$.

2.16. Digression ? Produits scalaires du plan

Ce paragraphe apparemment digressif décrit un espace métrique qui va se révéler être isométrique à $\mathscr{H}$. Reprenons la situation de [H2G2, exercice II-F.22]. Soit $\mathscr{S}_2^{++}(\mathbb{R})$ le cône des matrices 2×2 symétriques réelles définies

positives, c'est-à-dire l'ensemble des produits scalaires euclidiens sur $\mathbb{R}^2$. Il admet une action naturelle de $\mathbb{R}^{+*}$ par multiplication. Il est d'usage d'appeler *structure conforme* une orbite pour cette action, c'est-à-dire un produit scalaire à constante près. On va identifier l'ensemble des structures conformes avec deux « modèles géométriques » : l'un, noté $\mathscr{C}_2$, est l'intérieur d'une parabole et l'autre est $\mathscr{H}$. Tous deux sont munis d'une distance qui s'exprime en termes de birapport, et la bijection entre eux est une isométrie. Ce qui est remarquable, c'est que le groupe projectif qui agit est $\mathrm{PSL}_2(\mathbb{C})$ dans un cas, $\mathrm{PGL}_3(\mathbb{R})$ dans l'autre.

Un produit scalaire est décrit par sa matrice dans la base canonique de $\mathbb{R}^2$:

$$A = \begin{pmatrix} a & b \\ b & d \end{pmatrix}, \quad \text{où } a, b, d \in \mathbb{R},\ a + d > 0 \text{ et } ad - b^2 > 0.$$

L'orbite $\mathbb{R}^{+*}A$ contient un unique produit scalaire pour lequel le premier vecteur de la base canonique a pour norme 1, c'est $a^{-1}A$. On peut donc identifier $\mathscr{S}_2^{++}/\mathbb{R}^{+*}$ à l'intérieur d'une parabole :

$$\mathscr{C}_2 = \{(b, d) \in \mathbb{R}^2,\ d - b^2 > 0\}.$$

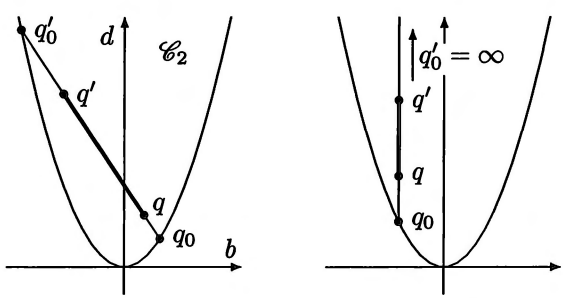


Figure 2.4. *Distance de Hilbert dans* $\mathscr{C}_2$

L'intérêt de cette description, c'est que $\mathscr{C}_2$ est un convexe du plan qui ne contient aucune droite : on peut donc le munir de la distance de Hilbert $D_{\mathscr{C}_2}$. Rappelons sa définition. Soient q et q' deux points de $\mathscr{C}_2$. Si elle n'est pas verticale, la droite (qq') coupe le bord de $\mathscr{C}_2$ en deux points q_0 et q_0', nommés de sorte à avoir dans l'ordre q_0, q, q', q_0'. Si la droite (qq') est verticale, l'intersection manquante devient ∞ (figure 2.4). On pose alors dans les deux cas : $D_{\mathscr{C}_2}(q, q') = \ln[q, q', q_0', q_0]$. On a vu au [H2G2, § X-2.3] que c'est une distance.

De plus, l'action du groupe $\mathrm{SL}_2(\mathbb{R})$ sur $\mathscr{S}_2^{++}$ par congruence en induit une de $\mathrm{PSL}_2(\mathbb{R})$ sur le quotient[8] $\mathscr{S}_2^{++}/\mathbb{R}^{+*}$ et donc sur $\mathscr{C}_2$ par transport. Décrivons-la.

[8]Comme PSL_2 est le quotient de SL_2 par $\{\pm \mathrm{I}_2\}$, le groupe PSL_2 agit déjà sur $\mathscr{S}_2^{++}$.

2.17. Lemme. *Le groupe* $\mathrm{PSL}_2(\mathbb{R})$ *agit sur l'ensemble* $\mathscr{C}_2$ *par des homographies (au sens du plan projectif réel) ; en particulier, il préserve la distance de Hilbert.*

Démonstration. L'action de $\mathrm{PSL}_2(\mathbb{R})$ par congruence sur l'espace $\mathscr{S}_2$ des matrices symétriques réelles est linéaire et elle préserve la signature par [H2G2, théorème V-1.2 (ii)], donc le cône des formes euclidiennes $\mathscr{S}_2^{++}$. Plaçons-nous dans le système de coordonnées (a, b, d) de $\mathscr{S}_2$ défini par l'écriture d'une matrice symétrique sous la forme

$$\begin{pmatrix} a & b \\ b & d \end{pmatrix}.$$

Le complémentaire de la droite projective d'équation $a = 0$ dans $\mathbb{P}(\mathscr{S}_2)$ s'identifie avec le plan affine d'équation $a = 1$ dans $\mathscr{S}_2 = \mathbb{R}^3$. De la sorte, on retrouve l'identification de $\mathscr{S}_2^{++}/\mathbb{R}^{+*}$ à $\mathscr{C}_2$, ce qui donne une action de $\mathrm{PSL}_2(\mathbb{R})$ sur $\mathscr{C}_2$.

Comme $\mathrm{PSL}_2(\mathbb{R})$ agit sur l'espace $\mathscr{S}_2$ de façon linéaire, il agit sur le plan projectif $\mathbb{P}(\mathscr{S}_2)$ par des homographies (au sens de [4, § VI.5]. De façon plus explicite, l'action sur $\mathscr{C}_2$ est décrite ainsi : pour

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \quad \text{et } q = \begin{pmatrix} 1 & b \\ b & d \end{pmatrix} \in \mathscr{C}_2,$$

on calcule :

$$g \cdot q = g q\, {}^t g = \begin{pmatrix} a' & b' \\ b' & d' \end{pmatrix} \quad \text{où} \quad \begin{cases} a' = \alpha^2 + 2\alpha\beta b + \beta^2 d \\ b' = \alpha\gamma + (\alpha\delta + \beta\delta)b + \beta\delta d \\ d' = \gamma^2 + 2\gamma\delta b + \delta^2 d, \end{cases}$$

de sorte que l'action sur $\mathscr{C}_2$ s'exprime ainsi :

$$g \cdot (b, d) = \left(\frac{\alpha\gamma + (\alpha\delta + \beta\delta)b + \beta\delta d}{\alpha^2 + 2\alpha\beta b + \beta^2 d}, \frac{\gamma^2 + 2\gamma\delta b + \delta^2 d}{\alpha^2 + 2\alpha\beta b + \beta^2 d} \right),$$

ce qui est bien une homographie du plan réel, *i.e.* un élément de $\mathrm{PGL}_3(\mathbb{R})$!

Vu la façon dont est définie la distance de Hilbert, elle est invariante par toute transformation qui préserve l'alignement et le birapport, si bien que $\mathrm{PSL}_2(\mathbb{R})$ agit sur $\mathscr{C}_2$ par isométries. □

2.18. Remarque. À la place du plan $a = 1$, on aurait pu en choisir un autre qui coupe le cône $\mathscr{S}_2^{++}$; au lieu de $\mathscr{C}_2$, on aurait trouvé l'intérieur d'une autre conique : la distance obtenue sur $\mathscr{S}_2^{++}/\mathbb{R}^{+*}$ aurait été la même puisqu'un isomorphisme linéaire qui envoie un plan sur l'autre induit une homographie entre ces deux plans, ce qui préserve la distance de Hilbert.

2.19. Produits scalaires du plan et demi-plan de Poincaré

Même pour un produit scalaire euclidien, le cône isotrope reste un invariant important ! Ici, il fournit un lien naturel entre l'ensemble des structures conformes et le demi-plan de Poincaré. Bien sûr, il faut chercher les points isotropes non nuls à coefficients complexes : il s'agit essentiellement des *points cycliques* de [4, définition VII.5.5].

On part de la forme euclidienne q sur $\mathbb{R}^2$ ayant pour matrice la matrice A ci-dessus. On a déjà dit que a n'est pas nul. On étend q en une forme bilinéaire sur $\mathbb{C}^2$. Pour un vecteur (x,y) de $\mathbb{C}^2$, on écrit classiquement :

$$\begin{aligned} q(x,y) &= ax^2 + 2bxy + dy^2 = a\left(\left(x + \frac{b}{a}y\right)^2 + \frac{ad-b^2}{a^2}y^2\right) \\ &= \frac{1}{a}\left(ax + \left(b + i\sqrt{ad-b^2}\right)y\right)\left(ax + \left(b - i\sqrt{ad-b^2}\right)y\right) \end{aligned}$$

Ainsi, le cône isotrope de q étendue à $\mathbb{C}^2$ est formé de deux droites correspondant aux points de $\mathbb{P}^1(\mathbb{C})$ ayant pour coordonnées homogènes :

$$\left[-b + i\sqrt{ad-b^2} : a\right] \quad \text{et} \quad \left[-b - i\sqrt{ad-b^2} : a\right].$$

En notant $[x:y]$ les coordonnées homogènes dans $\mathbb{P}^1$, ces deux points sont dans l'ouvert défini par $y \neq 0$, identifié à $\mathbb{C}$ via $\mathbb{C} \to \mathbb{P}^1(\mathbb{C})$, $x \mapsto [x:1]$. Les deux complexes correspondants sont conjugués l'un de l'autre, on va sélectionner celui qui a une partie imaginaire positive.

De façon plus terre à terre, on associe à la forme euclidienne q l'unique $z \in \mathscr{H}$ tel que $q(z,1) = 0$: il ne dépend que de $\mathbb{R}^{+*}q$. Partant de la forme ayant pour coefficient $a = 1$, c'est-à-dire d'un point de $\mathscr{C}_2$, cela donne une bijection PC (*point cyclique*) dont on calcule la réciproque :

$$\begin{cases} \text{PC} : (b,d) \in \mathscr{C}_2 \longmapsto -b + i\sqrt{d-b^2} \in \mathscr{H} \\ \text{et} \quad x + iy \in \mathscr{H} \longmapsto (-x, x^2+y^2) \in \mathscr{C}_2. \end{cases}$$

2.20. Proposition. *L'application* PC *est une isométrie de l'ensemble des structures conformes (avec la distance $D_{\mathscr{C}_2}/2$, où $D_{\mathscr{C}_2}$ est la distance de Hilbert sur $\mathscr{C}_2$) vers le demi-plan de Poincaré (avec la distance hyperbolique).*

Démonstration. Soient (b,d) et (b',d') deux points de $\mathscr{C}_2$. On note z et z' leurs images par PC dans $\mathscr{H}$ (figure 2.5).

Supposons d'abord que $b = 0 = b'$, c'est-à-dire que les matrices des produits scalaires correspondants soient diagonales, et par exemple que $0 < d < d'$. Alors la droite contenant $(0,d)$ et $(0,d')$ coupe le bord de $\mathscr{C}_2$ en $(0,0)$ et

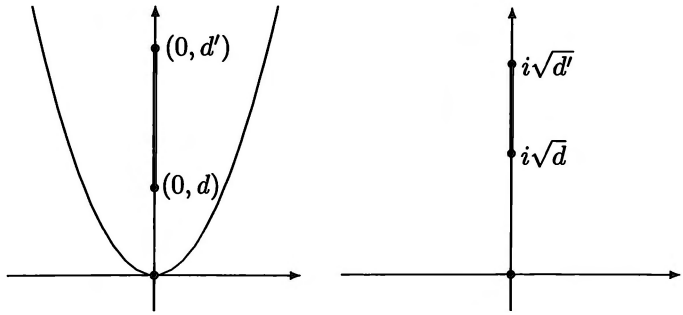


Figure 2.5. *Une géodésique particulière vue dans $\mathscr{C}_2$ et dans $\mathscr{H}$*

une demi-droite entière est contenue dans $\mathscr{C}_2$. Ainsi :

$$D_{\mathscr{C}_2}\big((0,d),(0,d')\big) = \ln[d,d',\infty,0] = \ln\frac{d'}{d}.$$

D'autre part, on a : $\mathrm{PC}(0,d) = i\sqrt{d}$ et $\mathrm{PC}(O,d') = i\sqrt{d'}$, d'où :

$$D_{\mathscr{H}}\big(i\sqrt{d}, i\sqrt{d'}\big) = \ln\big[i\sqrt{d}, i\sqrt{d'}, \infty, 0\big] = \ln\frac{i\sqrt{d'}}{i\sqrt{d}} = \frac{1}{2}\ln\frac{d'}{d}.$$

Cela prouve l'assertion dans le cas où $b = b' = 0$. Pour le cas général, on va utiliser une propriété d'équivariance de PC.

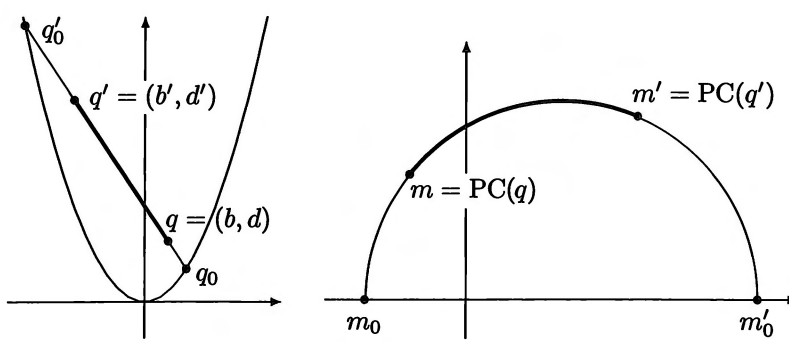


Figure 2.6. *Une géodésique générique vue dans $\mathscr{C}_2$ et dans $\mathscr{H}$*

Pour $A = \left(\begin{smallmatrix} 1 & b \\ b & d \end{smallmatrix}\right)$, $Z \in \mathbb{C}^2$ et $g \in \mathrm{SL}_2(\mathbb{R})$, on a :

$$^tZAZ = 0 \iff {}^t\big({}^tg^{-1}Z\big)\, gA\, {}^tg\,\big({}^tg^{-1}Z\big) = 0.$$

Or, l'image $\mathrm{PC}(b,d)$ est l'unique z de $\mathscr{H}$ tel que $^tZAZ = 0$, où $Z = \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$. Ainsi, le vecteur $Z' = {}^tg^{-1}Z$ est isotrope pour $gA\,{}^tg$. Notons-le $Z' = \left(\begin{smallmatrix} z' \\ w' \end{smallmatrix}\right)$. Alors, $\mathrm{PC}(g\cdot(b,d))$ est z'/w' ou son conjugué. Mais $z'/w' = {}^tg^{-1}\cdot z$ (voir

[H2G2, § X-1.2]) qui appartient donc à $\mathscr{H}$. Ainsi :

$$\mathrm{PC}\big(g\cdot(b,d)\big) = {}^t g^{-1}\cdot \mathrm{PC}(b,d).$$

À présent, par le théorème diagonalisation simultanée des matrices symétriques réelles définies positives, il existe g dans $\mathrm{SL}_2(\mathbb{R})$ dont les colonnes forment une base orthonormée pour les produits scalaires associés à (b,d) et (b',d'). On a donc, pour $\widehat{d}$ et $\widehat{d'}$ réels convenables : $g\cdot(b,d) = (0,\widehat{d})$ et $g\cdot(b',d') = (0,\widehat{d'})$. On a alors :

$$\begin{aligned} D_{\mathscr{C}_2}\big((b,d),(b',d')\big) &= D_{\mathscr{C}_2}\big(g\cdot(b,d), g\cdot(b',d')\big) = D_{\mathscr{C}_2}\big((0,\widehat{d}),(0,\widehat{d'})\big) \\ &= 2D_{\mathscr{H}}\big(\mathrm{PC}(0,\widehat{d}),\mathrm{PC}(0,\widehat{d'})\big) = 2D_{\mathscr{H}}\big({}^t g^{-1}\cdot\mathrm{PC}(b,d), {}^t g^{-1}\cdot\mathrm{PC}(b',d')\big) \\ &= 2D_{\mathscr{H}}\big(\mathrm{PC}(b,d),\mathrm{PC}(b',d')\big). \end{aligned}$$

2.21. Cinq modèles du plan hyperbolique

Par *plan hyperbolique*, on désigne n'importe quel espace isométrique à $\mathscr{H}$. On dit que $\mathscr{H}$ et $\mathscr{C}_2$ en sont des modèles. Par identification, les structures conformes $\mathscr{S}_2^{++}/\mathbb{R}^{+*}$ en forment un aussi, mais il est un peu abstrait. On va en ajouter trois sans preuves pour aboutir à la figure 2.1. On part de $\mathscr{S}_2 \simeq \mathbb{R}^3$. La matrice

$$\begin{pmatrix} a & b \\ b & d \end{pmatrix}$$

est définie positive si et seulement si $a>0$ et $ad-b^2>0$. Alors, $\mathscr{S}_2^{++}/\mathbb{R}^{+*}$ est l'ensemble des demi-droites de $\mathscr{S}_2$ qui sont à l'intérieur du cône isotrope du déterminant et dans le demi-espace $a>0$.

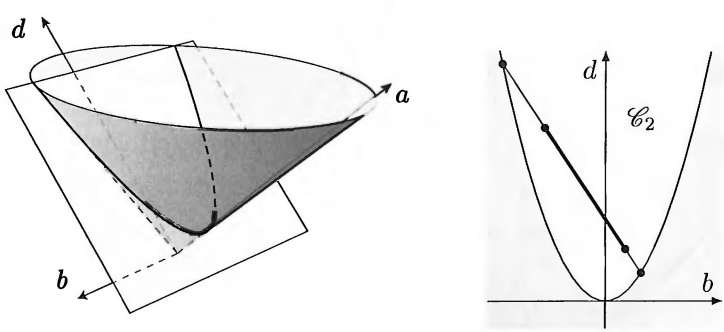


Figure 2.7. *Du cône à la parabole*

Chacune de ces demi-droites coupe le plan $a=1$ en un point unique, ce qui redonne le modèle de la parabole —l'identification $\mathscr{S}_2^{++}/\mathbb{R}^{+*} \to \mathscr{C}_2$ déjà exploitée. Mais l'on peut aussi associer à chaque demi-droite son point

d'intersection avec l'hyperboloïde d'équation det = 1, c'est-à-dire

$$\mathscr{Q} = \{(a,b,c) \in \mathbb{R}^3,\ ad - b^2 = 1\}.$$

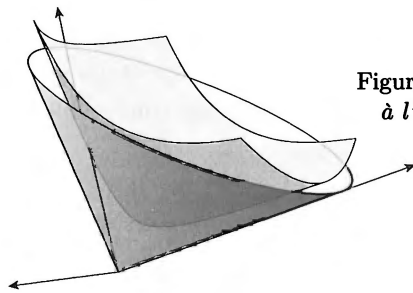


Figure 2.8. *Du cône à l'hyperboloïde*

Pour mieux voir cet hyperboloïde, on introduit de nouvelles coordonnées :

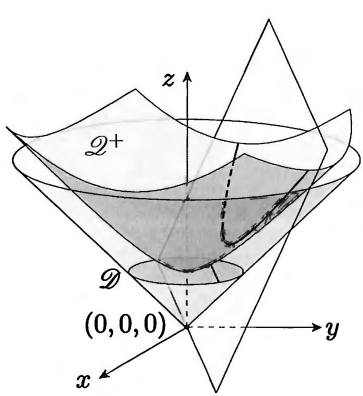
$$x = \frac{a-d}{2},\quad y = b,\quad z = \frac{a+d}{2}.$$

Si l'on rend ce repère orthonormé, $\mathscr{Q}$ est l'hyperboloïde de révolution :

$$x^2 + y^2 - z^2 = -1.$$

De la sorte, les structures conformes s'identifient à la nappe $\mathscr{Q}^+$ de l'hyperboloïde contenue dans le demi-espace $z > 0$. Avec un regard projectif, on voit de plus qu'une géodésique de $\mathscr{C}_2$ s'identifie à l'intersection de la nappe $\mathscr{Q}^+$ avec un plan vectoriel.

Il est classique de transformer la nappe $\mathscr{Q}^+$ en le disque-unité $\mathscr{D}$ par projection centrale de centre l'origine $(0,0,0)$ sur le plan d'équation $z = 1$, soit $a+d = 2$. On retrouve ainsi le « modèle de Klein » du plan hyperbolique, où les géodésiques sont des segments de droites et la distance, celle de Hilbert. Ce modèle s'obtient à partir de la parabole par une homographie (du plan projectif réel), que l'on pourra expliciter.



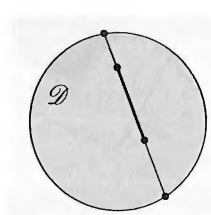
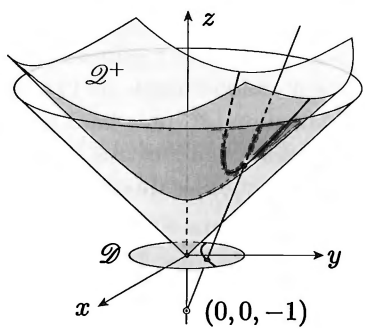


Figure 2.9. *De l'hyperboloïde au disque de Klein*

Une autre projection centrale envoie $\mathscr{Q}^+$ vers le disque de Poincaré $\mathscr{D}$: c'est la projection de centre $(x,y,z) = (0,0,-1)$ ou $(a,b,d) = (-1,0,-1)$ sur le plan $z = 0$. Cette transformation envoie les géodésiques de $\mathscr{Q}^+$, c'est-à-dire l'intersection de $\mathscr{Q}^+$ avec les plans contenant l'origine, sur des cercles orthogonaux au cercle-unité. Géométriquement, ce n'est pas évident.



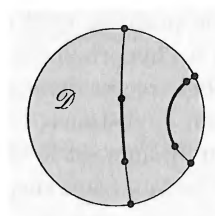


Figure 2.10. *De l'hyperboloïde au disque de Poincaré (et une géodésique gratuite)*

Pour fermer la boucle, l'homographie $H\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, $z \mapsto (z-i)/(z+i)$ envoie l'axe réel, qui est la médiatrice du segment $[i,-i]$, sur le cercle-unité ; on en déduit que H envoie $\mathscr{H}$ sur le disque-unité $\mathscr{D}$. Les géodésiques de $\mathscr{H}$ sont envoyées sur les cercles qui, puisque H est holomorphe donc conforme, sont orthogonaux au cercle-unité. Deux points distincts de $\mathscr{D}$ appartiennent à un unique cercle orthogonal au cercle-unité, car la même propriété est vraie dans $\mathscr{H}$. Par préservation du birapport par H, on peut définir une métrique avec une formule analogue à celle que l'on utilise sur $\mathscr{H}$.

En fait, cette distance provient d'une métrique que l'on peut calculer en transportant celle de $\mathscr{H}$ via H et qui vaut :

$$\frac{\mathrm{d}x^2 + \mathrm{d}y^2}{\big(1-(x^2+y^2)\big)^2} = \frac{\mathrm{d}z\,\mathrm{d}\overline{z}}{(1-|z|^2)^2}.$$

C'est le disque de Poincaré, notre dernier modèle du plan hyperbolique.

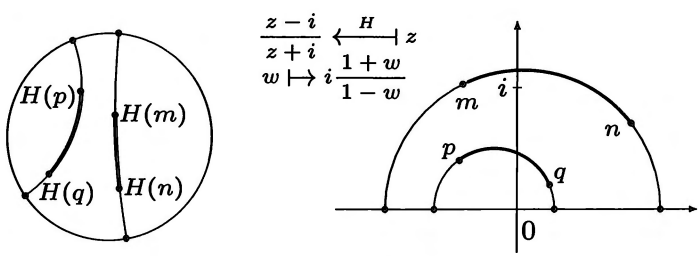


Figure 2.11. *Du disque au demi-plan de Poincaré*

2.22. Remarque (Pour quelques modèles de plus). Notre dernier modèle, certes, mais d'autres en préfèrent d'autres ! Prenons un point $p = (x, y, z)$ sur l'hyperboloïde d'équation $x^2 + y^2 - z^2 = 1$. Le plan tangent à p est l'orthogonal de p pour la forme quadratique hyperbolique $Q = x^2 + y^2 - z^2$. Or, la norme hyperbolique $Q(p)$ est strictement négative (c'est -1 !). Donc, par le théorème de Sylvester, la restriction de Q à $p^\perp$ est définie positive. Cela donne une notion de longueur pour les vecteurs tangents à l'hyperboloïde et, partant, une façon de mesurer les longueurs des courbes tracées dessus. On obtient sur chaque nappe de l'hyperboloïde une notion de distance, comme on l'a fait dans $\mathscr{H}$ plus haut : la distance entre deux points est la borne inférieure des longueurs des courbes qui les relient. C'est un (sans surprise ?) un nouveau modèle du plan hyperbolique.

On montre avec le théorème de Witt que le groupe $\mathrm{SO}_0(2,1)$ agit transitivement sur chaque nappe de l'hyperboloïde ; de plus, le stabilisateur d'un point est isomorphe à $\mathrm{SO}_0(2,0) \simeq \mathrm{SO}_2(\mathbb{R})$. C'est, dans la théorie de Lie, l'un des premiers exemples d'*espaces symétriques.*

3. Un arbre pour les triplets pythagoriciens

Nous mettons ici une structure d'arbre ternaire sur l'ensemble des triplets pythagoriciens. Cet arbre est obtenu par recollement à partir d'une variante du graphe de Cayley d'un sous-groupe libre[9] de $\mathrm{PSL}_2(\mathbb{Z})$.

Un groupe libre

3.1. Notations. On appelle $\Gamma(2)$ le sous-groupe de $\mathrm{PGL}_2(\mathbb{C})$ engendré par les homographies u et v suivantes :

$$\forall z \in \mathbb{P}^1(\mathbb{C}), \quad u(z) = z + 2 \quad \text{et} \quad v(z) = \frac{z}{2z+1}.$$

3.2. Proposition. *Le groupe $\Gamma(2)$, engendré par u et v, est isomorphe au groupe libre à deux générateurs.*

Introduisons quatre disques[10] ouverts dans $\mathbb{P}^1(\mathbb{C})$:

$$\begin{cases} P^- = \{z \in \mathbb{C},\ \mathrm{Re}(z) < -1\}, \\ P^+ = \{z \in \mathbb{C},\ \mathrm{Re}(z) > 1\}, \\ P_0 = \{z \in \mathbb{C},\ -1 < \mathrm{Re}(z) < 1\}, \end{cases} \qquad \begin{cases} Q^- = \left\{z \in \mathbb{C}, \left|z + \frac{1}{2}\right| < \frac{1}{2}\right\}, \\ Q^+ = \left\{z \in \mathbb{C},\ \left|z - \frac{1}{2}\right| < \frac{1}{2}\right\}, \\ Q_0 = \mathbb{C} \setminus \overline{Q^+ \cup Q^-}. \end{cases}$$

On désignera par F l'intérieur du complémentaire de la réunion de ces quatre disques, c'est-à-dire la partie en blanc de la figure 3.1.

[9] Pour des informations sur les groupes libres, voir l'annexe I-B.

[10] Dans la droite $\mathbb{P}^1(\mathbb{C})$, qui est une sphère, $P^\pm$ et $Q^\pm$ sont bien des disques...

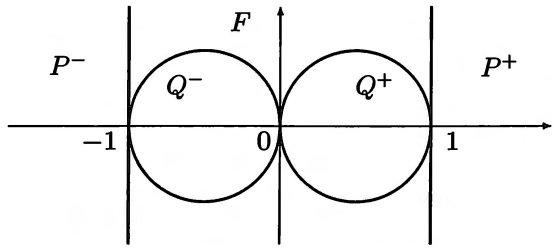


Figure 3.1. *Mise en place du ping-pong*

3.3. Lemme (« du ping-pong »). *Avec les notations ci-dessus :*

(i) *l'homographie u envoie le complémentaire de $\overline{P^-}$ dans P^+ ;*
(ii) *son inverse u^{-1} envoie le complémentaire de $\overline{P^+}$ dans P^- ;*
(iii) *l'homographie v envoie le complémentaire de $\overline{Q^-}$ dans Q^+ ;*
(iv) *l'homographie v envoie le complémentaire de $\overline{Q^+}$ dans Q^-.*

Démonstration (du lemme). Les deux premières assertions sont évidentes. Pour prouver les deux autres, on introduit $\iota : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, $z \mapsto z^{-1}$. On vérifie que $\iota u \iota^{-1} = v$: pour $z \in \mathbb{P}^1(\mathbb{C})$, on a en effet :

$$\iota u \iota^{-1}(z) = \frac{1}{\frac{1}{z} + 2} = \frac{z}{2z+1}.$$

Pour $s \in \mathbb{R}^*$, l'image de la droite $D_s = \{\mathrm{Re}(z) = s\}$ par ι est le cercle C_s de diamètre $[0, s^{-1}]$. En effet, sachant que l'image d'un cercle-droite par une homographie en est un autre, il suffit de montrer que $\iota(D_s) \subset C_s$; or, si $z = s + it$ avec $t \in \mathbb{R}$, on a :

$$\left|\iota(z) - \frac{1}{2s}\right| = \left|\frac{s - it}{2s(s+it)}\right| = \frac{1}{2|s|}.$$

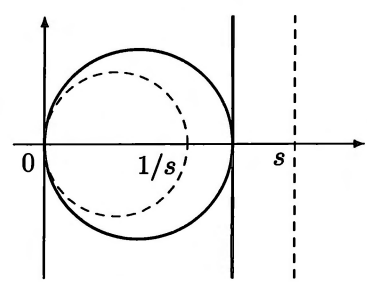


Figure 3.2. *Image de P^+ par ι*

Comme P^+ est la réunion des D_s ($s > 1$) et que Q^+ est la réunion des C_s ($s > 1$), on a : $\iota(P^+) = Q^+$. On prouverait de même que $\iota(P^-) = Q^-$. Enfin, ι est involutive. Le principe de conjugaison nous permet de déduire les deux dernières assertions.

□

Démonstration (de la proposition). Soit $n \in \mathbb{N}^*$, soit $(w_1, \ldots, w_n) \in \{u, v\}^n$ et soit $(k_1, \ldots, k_n) \in (\mathbb{Z} \setminus \{0\})^n$ tels que $w_i \neq w_{i+1}$ pour tout i ; on pose $g = w_1^{k_1} w_2^{k_2} \cdots w_n^{k_n}$. On doit démontrer que $g \neq \mathrm{Id}$.

Pour cela, fixons $z \in F$. Supposons que $w_n = u$. Alors, $u^{k_n}(z)$ appartient à P^+ (si $k_n > 0$) ou à P^- (si $k_n < 0$). Par conséquent, $v^{k_{n-1}} u^{k_n}(z)$ appartient

à Q^+ (si $k_{n-1} > 0$) ou à Q^- (si $k_{n-1} < 0$), et ainsi de suite. De proche en proche, on en déduit que $g(z)$ appartient à l'un des quatre disques P^+, P^-, Q^+, Q^-. On traiterait de même le cas $w_n = v$. Comme z appartient à F, cela implique que $g(z) \neq z$, c'est-à-dire que $g \neq \mathrm{Id}$. La proposition en résulte. □

3.4. Remarque. L'argument de la preuve est appelé « argument du *ping-pong* ». Au départ, la balle est dans F ; l'action d'un mot non trivial en u et v établit un jeu de ping-pong entre $P^+ \cup P^-$ et $Q^+ \cup Q^-$. En tout état de cause, on ne reviendra jamais dans F.

Deuxième réalisation de $\Gamma(2)$

3.5. Proposition. *Le groupe* $\Gamma(2)$ *est le noyau du morphisme naturel* $\mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z})$. *En particulier, il est d'indice* 6 *dans* $\mathrm{PSL}_2(\mathbb{Z})$.

Démonstration. Soit K le noyau de la réduction modulo 2. Bien sûr, u et v appartiennent à K ; comme $-1 \equiv 1 \pmod 2$, la matrice $-\mathrm{I}_2$ aussi. L'image réciproque de K dans $\mathrm{SL}_2(\mathbb{Z})$ est :

$$\tilde{\Gamma}(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ a \equiv d \equiv 1 \pmod 2,\ \ b \equiv c \equiv 0 \pmod 2 \right\}.$$

Le diagramme suivant est commutatif :

$$\begin{array}{ccccc} \tilde{\Gamma}(2) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \\ \downarrow & & \downarrow & & \| \\ K & \longrightarrow & \mathrm{PSL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}). \end{array}$$

Pour prouver la proposition, il suffit donc de montrer que le groupe $\tilde{\Gamma}(2)$ est engendré par

$$-\mathrm{I}_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Soit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{\Gamma}(2).$$

On montre par récurrence sur $\delta(A) = \max(|a|, |c|)$ que A appartient au groupe engendré par $-\mathrm{I}_2$, U et V.

Si $\delta(A) = 1$, les conditions de parité font que $|a| = 1$ et $c = 0$. Mais alors, comme le déterminant de A vaut 1, on a : $d = a$ et $A = \pm U^{b/2}$.

Supposons que $\delta(A) \geqslant 2$. On calcule :

$$U^{\pm 1}A = \begin{pmatrix} a \pm 2c & b \pm 2d \\ c & d \end{pmatrix}, \quad V^{\pm 1}A = \begin{pmatrix} a & b \\ c \pm 2a & d \pm 2b \end{pmatrix}.$$

On a : $a \neq 0$, car a est impair ; $c \neq 0$, car sinon, l'égalité $1 = \det(A) = ad$ force $\delta(A) = 1$; $|a| \neq |c|$, par raison de parité.

Or, si $0 < |c| < |a|$, alors $-|a| < |a| - 2|c| < |a|$, d'où : $\big||a| - 2|c|\big| < |a| = \max(|a|, |c|)$. Alors, si a et c sont de même signe, on a : $\delta(U^{-1}A) < \delta(A)$; sinon, on a : $\delta(UA) < \delta(A)$.

De même, si $0 < |a| < |c|$, on a $\big||c| - 2|a|\big| < |c| = \max(|a|, |c|)$. Si a et c sont de même signe, on a : $\delta(V^{-1}A) < \delta(A)$; sinon, on a : $\delta(VA) < \delta(A)$. On peut donc conclure la récurrence. □

Énumération des triplets pythagoriciens par un arbre

On appellera *triplet pythagoricien* un triplet d'entiers $(x, y, z) \in \mathbb{Z}^3$ tels que $x^2 + y^2 = z^2$. On ne fera pas la différence entre deux triplets dont seuls les signes changent et, par abus, ce que l'on appellera triplet est une classe d'équivalence de triplets. On dit qu'un triplet pythagoricien est *primitif* si les entiers qui le constituent sont deux à deux premiers entre eux. La description suivante est bien connue.

3.6. Proposition. *Tout triplet pythagoricien est multiple d'un triplet primitif. Tout triplet primitif est, aux signes et à permutation de x et y près, de la forme $(m^2 - n^2, 2mn, m^2 + n^2)$, où m et n sont des entiers naturels premiers entre eux et de parités différentes, uniques à l'ordre près.*

Démonstration. Soit (x, y, z) un triplet pythagoricien. Quitte à diviser par le pgcd de x, y et z, on peut les supposer premiers entre eux dans leur ensemble. Mais si un nombre premier divise deux de ces trois entiers, (par exemple x et z), il divise aussi le carré du troisième (dans l'exemple, $y^2 = z^2 - x^2$), donc il divise le troisième y. Ainsi, x, y et z sont deux à deux premiers entre eux. Cela prouve la première assertion.

Quitte à permuter x et y, on peut supposer que x est impair et y pair, ou l'inverse. En effet, si x et y étaient tous deux pairs, z le serait aussi, ce qui est exclu car le triplet est primitif. Si x et y étaient tous deux impairs, z serait pair et, par réduction modulo 4, les congruences $x^2 \equiv y^2 \equiv 1 \pmod 4$ et $z^2 \equiv 0 \pmod 4$ donneraient : $2 \equiv 0 \pmod 4$, ce qui est absurde.

On a : $y^2 = (z+x)(z-x)$. Si un entier naturel d divise $z+x$ et $z-x$, alors d divise $2z$ et $2x$; vu que z et x sont premiers entre eux, d divise 2 ; or, $z+x$ et $z-x$ sont pairs. Ainsi, leur PGCD est 2 et les entiers $k = (z+x)/2$ et $\ell = (z-x)/2$ sont premiers entre eux. Par l'égalité $(y/2)^2 = k\ell$, et le lemme de Gauss, k et ℓ sont des carrés, disons $k = m^2$ et $\ell = n^2$. Il vient alors : $x = m^2 - n^2$, $z = m^2 + n^2$, puis $y = 2mn$. Comme x est impair, m et n sont de parités différentes.

Pour l'unicité, il suffit de montrer que si $(m^2 - n^2, 2mn) = (m'^2 - n'^2, 2m'n')$, alors $m = \pm m'$ et $n = \pm n'$, ce qui résulte du constat[11] : $m^2 - n^2 + 2mni = (m + in)^2$. □

[11] Ce constat rappelle une autre stratégie de résolution, classique aussi, qui part de l'égalité $x^2 + y^2 = (x + iy)(x - iy)$ et utilise la factorialité de $\mathbb{Z}[i]$ au lieu de celle de $\mathbb{Z}$.

Lien avec $\Gamma(2)$

Les (classes de) triplets primitifs sont donc codé(e)s par un couple (m, n) formé d'un entier impair et d'un entier pair et premiers entre eux. À présent, on considère ${}^t(m\ n)$ comme la première colonne d'un élément de $\tilde{\Gamma}(2)$, avant de passer dans $\Gamma(2)$.

On rappelle que la matrice U, qui relève l'homographie $z \mapsto z+2$, a été définie dans la preuve de la proposition 3.5.

3.7. Lemme. *Soient m et n deux entiers premiers entre eux, m impair, n pair. Il existe p, q entiers tels que $A = \begin{pmatrix} m & p \\ n & q \end{pmatrix} \in \tilde{\Gamma}(2)$. De plus, les autres matrices de cette forme sont les matrices AU^k ($k \in \mathbb{Z}$).*

Démonstration. D'après la relation de Bézout, on peut trouver p et q entiers tels que $mq - np = 1$. Comme n est pair, q est impair. Si p est pair, on a gagné ; sinon, on pose $p' = p + m$ et $q' = q + n$; ainsi, p' est pair, q' est impair et l'on a : $mq' - np' = 1$. Cela prouve l'existence.

Supposons que les matrices $A = \begin{pmatrix} m & p \\ n & q \end{pmatrix}$ et $A' = \begin{pmatrix} m & p' \\ n & q' \end{pmatrix}$ appartiennent toutes deux à $\tilde{\Gamma}(2)$. En comparant leur déterminant, on trouve : $m(q' - q) = n(p - p')$. D'après le lemme de Gauss, il existe un entier j tel que $p - p' = jm$. Comme p, p' et m sont impairs, j est pair, disons $j = 2k$. Il vient : $p' = p + 2km$ et $q' = q + 2kn$, ce qui exprime que l'on a : $A' = AU^k$. Inversement, pour tout k, A et AU^k ont la même première colonne. □

3.8. Notations. Soit D la matrice diagonale dont les coefficients diagonaux sont -1 et 1, et soit Φ la conjugaison par D : comme D est d'ordre 2 dans $\mathrm{GL}_2(\mathbb{Z})$ et que $\mathrm{SL}_2(\mathbb{Z})$ est distingué dans $\mathrm{GL}_2(\mathbb{Z})$, Φ est une involution de $\tilde{\Gamma}(2)$. Vu que D commute à $-\mathrm{I}_2$, la conjugaison Φ induit une involution φ de $\Gamma(2)$. C'est l'automorphisme caractérisé par

$$\varphi(u) = u^{-1}, \qquad \varphi(v) = v^{-1},$$

où u et v sont les générateurs de $\Gamma(2)$ définis en 3.1.

3.9. Lemme

(i) *L'application $F : \tilde{\Gamma}(2) \to \mathscr{T}$, $\begin{pmatrix} m & n \\ p & q \end{pmatrix} \mapsto (m^2 - n^2, 2mn, m^2 + n^2)$ induit par passage au quotient une surjection $f : \Gamma(2) \to \mathscr{T}$.*

(ii) *Pour $g, g' \in \Gamma(2)$, on a :*

$$f(g) = f(g') \iff \exists k \in \mathbb{Z},\ g' = gu^k \text{ ou } g' = \varphi(gu^k).$$

3.10. Exemple. On a : $f(\mathrm{Id}) = f(u^k) = (1, 0, 1)$ pour tout k ; $f(v) = (3, 4, 5)$; $f(uv) = (21, 20, 29)$; $f(v^2) = (15, 8, 17)$; $f(u^{-1}v) = (5, 12, 13)$...

Démonstration. (i) Comme $F(A) = F(-A)$ pour tout $A \in \tilde{\Gamma}(2)$, cela a un sens de définir $f(g) = F(A)$ si A est une des deux matrices qui représentent une homographie $g \in \Gamma(2)$. D'après la proposition 3.6 et du lemme 3.7 (i), F est surjective et f l'est donc aussi.

(ii) La proposition 3.6 montre également que si deux éléments A et A' de $\tilde{\Gamma}(2)$ sont associés au même triplet primitif, alors les premières colonnes de A et A' coïncident aux signes près. Or, on a :

$$\Phi(A) = DAD^{-1} = \begin{pmatrix} m & -p \\ -n & q \end{pmatrix} \quad \text{si } A = \begin{pmatrix} m & p \\ n & q \end{pmatrix}.$$

Ainsi, on a : $F(A) = F(A')$ si et seulement si les premières colonnes de A' et $\varepsilon\Phi^\delta(A)$ coïncident, pour $\varepsilon \in \{-1, 1\}$ et $\delta \in \{0, 1\}$ convenables ; d'après l'assertion (ii) du lemme 3.7, cela signifie que $A' = \varepsilon\Phi^\delta(A)U^k$ pour un entier k convenable. Lorsque l'on passe à $\Gamma(2)$, le signe ε disparaît et Φ devient φ. □

Bien sûr, le triplet correspondant au neutre de $\Gamma(2)$ est le trivial $(1, 0, 1)$. En utilisant le fait que le groupe est libre, on obtient un paramétrage des triplets primitifs.

3.11. Lemme. *Aux signes et à permutation de x et y près, tout triplet primitif (x, y, z) non trivial ($xyz \neq 0$) est l'image par f d'un unique élément*

$$u^{k_1}v^{\ell_1}u^{k_2}v^{k_2}\cdots u^{k_s}v^{\ell_s},$$

où $s \geqslant 1$, $k_1 \in \mathbb{Z}$, $k_2, \ldots, k_s, \ell_1, \ldots, \ell_{s-1} \in \mathbb{Z}^*$ et $\ell_s \in \mathbb{N}^*$.

Démonstration. Existence. Fixons à cet effet un triplet primitif non trivial. D'après le lemme 3.9, il est de la forme $f(g)$ pour $g \in \Gamma(2)$ convenable. Comme $\Gamma(2)$ est engendré par u et v, on peut trouver $s \in \mathbb{N}$, $(w_1, \ldots, w_s) \in \{u, v\}^s$, avec $w_{i+1} \neq w_i$ pour tout i, et $(k_1, \ldots, k_s) \in \big(\mathbb{Z} \setminus \{0\}\big)^s$ tels que $g = w_1^{k_1} \cdots w_s^{k_s}$ (dire que $s = 0$, ce serait dire que $g = \mathrm{Id}$).

Il est impossible que g soit une puissance de u, c'est-à-dire que $s = 1$ et $w_1 = u$: sinon, on aurait $f(g) = f(u^{k_1}) = f(\mathrm{Id}) = (1, 0, 1)$, ce qui est exclu. Par suite, w_s ou w_{s-1} est v. Quitte à remplacer g par $g' = w_1^{k_1} \cdots w_{s-1}^{k_{s-1}}$, on peut supposer que $w_s = v$: en effet, on a : $f(g) = f(g'u^{k_s}) = f(g')$.

Quitte à remplacer g par $\varphi(g)$, on peut supposer que $k_s > 0$: en effet, on a clairement $\varphi(g) = w_1^{-k_1} \cdots w_s^{-k_s}$ et $f\big(\varphi(g)\big) = f(g)$.

Ainsi, g est un produit de puissances de u et de v qui se termine par une puissance positive de v. En d'autres termes, g s'écrit sous la forme $u^{k_1}v^{\ell_1}u^{k_2}v^{\ell_2}\cdots u^{k_s}v^{\ell_s}$, où $s \in \mathbb{N}^*$, $k_1 \in \mathbb{Z}$, $k_2, \ldots, k_s, \ell_1, \ldots, \ell_{s-1} \in \mathbb{Z} \setminus \{0\}$ et $\ell_s \in \mathbb{N}^*$.

Unicité. Supposons que deux éléments

$$g = u^{k_1}v^{\ell_1}u^{k_2}v^{k_2}\cdots u^{k_s}v^{\ell_s} \quad \text{et} \quad g' = u^{k'_1}v^{\ell'_1}u^{k'_2}v^{k'_2}\cdots u^{k'_{s'}}v^{\ell'_{s'}}$$

aient la même image par f. Alors, d'après le lemme 3.9, on a pour un entier k convenable : $g' = gu^k$ ou $g' = \varphi(gu^k) = \varphi(g)u^{-k}$. Comme $\Gamma(2)$ est libre, les écritures de g' et g sont uniques, ce qui donne : $k = 0$. Comme, de plus, φ change le signe de tous les exposants et que les deux exposants finaux ℓ_s et $\ell'_{s'}$ sont positifs, on a : $g' = g$. En utilisant à nouveau le fait que $\Gamma(2)$ est libre, on peut conclure. □

3.12. Notations. On note $\mathscr{V}$ l'ensemble des éléments de $\Gamma(2) = \langle u, v\rangle$ dont l'écriture réduite se termine par une puissance positive ou nulle de v. Les éléments de $\mathscr{V}$ sont reliés par les arêtes en gras dans la figure 3.3.

On reformule le dernier lemme.

3.13. Proposition. *L'application f induit une bijection de $\mathscr{V}$ sur l'ensemble des triplets primitifs.*

3.14. Définition (Graphe de Cayley (variante)). Dans ce paragraphe, on appellera *graphe de Cayley* de $\Gamma(2)$ le graphe dont les sommets sont les éléments de $\Gamma(2)$, dans lequel il y a une arête entre tout élément g et les quatre éléments ug, $u^{-1}g$, vg et $v^{-1}g$. ([12])

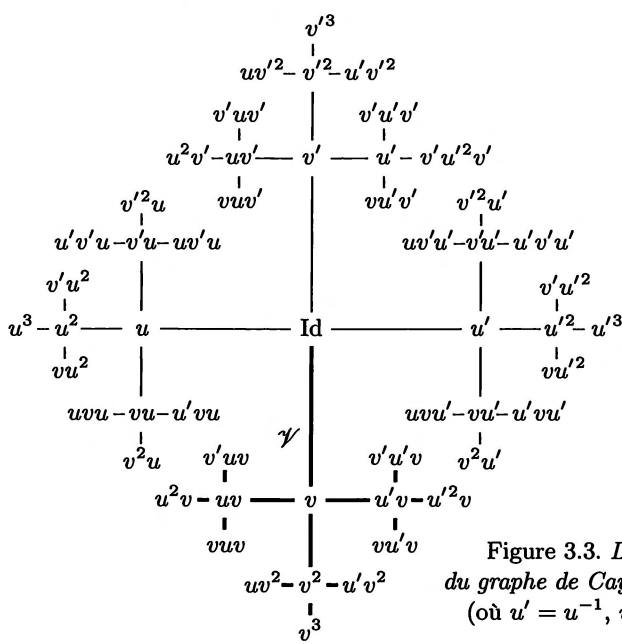


Figure 3.3. *Le début du graphe de Cayley de* $\Gamma(2)$ (où $u' = u^{-1}$, $v' = v^{-1}$)

[12] La convention habituelle consiste à multiplier par les générateurs à droite et pas à gauche comme ici.

Les éléments qui se terminent par une puissance positive ou nulle de v forment une branche $\mathscr{V}$ (en gras sur la figure 3.3).

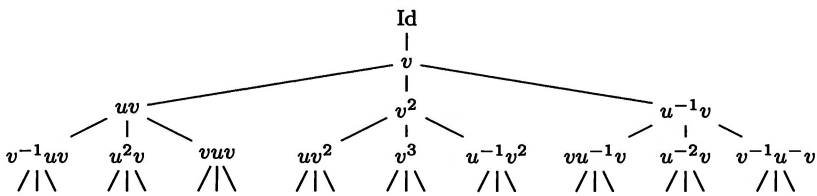


Figure 3.4. *La branche $\mathscr{V}$ de l'arbre de Cayley de $\Gamma(2)$*

3.15. Corollaire. *Par identification avec la branche $\mathscr{V}$ issue du neutre dans le graphe de Cayley de $\Gamma(2)$, l'ensemble des triplets primitifs est muni d'une structure d'arbre ternaire*[13] *(figure 3.5).*

3.16. Remarque. On peut alors obtenir la branche $\mathscr{V}$ par recollement à partir du graphe de Cayley de $\Gamma(2)$, en identifiant les différents sommets g, gu^k ($k \in \mathbb{Z}$) et $\varphi(g)u^\ell$ ($\ell \in \mathbb{Z}$). En effet, cette identification préserve la structure de graphe : deux sommets g et h sont reliés si et seulement s'il existe $w \in \{u^{\pm 1}, v^{\pm 1}\}$ tel que $g = wh$. C'est équivalent à $gu^k = whu^k$ et à $\varphi(g)u^\ell = w^{-1}\varphi(h)u^\ell$, c'est-à-dire à l'existence d'une arête entre gu^k et hu^k et entre $\varphi(g)u^\ell$ et $\varphi(h)^\ell$.

En d'autres termes, le groupe $G = \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ agit sur le graphe de Cayley $\mathscr{C}$ de $\Gamma(2)$ par automorphismes de graphes : un élément k de $\mathbb{Z}$ agit par translation à droite par u^k, l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ agit par φ. Le quotient $\mathscr{C}/G$ est encore un graphe, qui s'identifie à la branche $\mathscr{V}$ de $\mathscr{C}$. Cela revient en quelque sorte à réaliser $\mathscr{V}$ comme le « graphe de Cayley » de l'ensemble-quotient $\Gamma(2)/\langle u \rangle$.

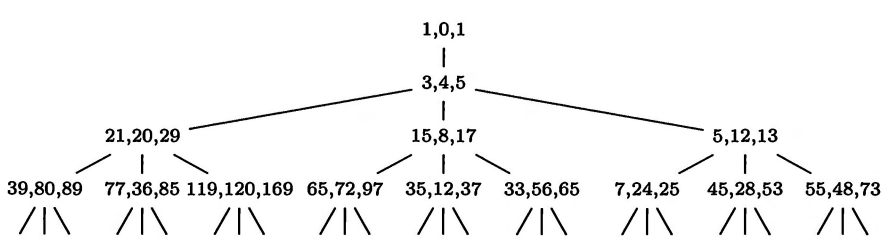


Figure 3.5. *Le début de l'arbre pythagoricien*

[13] Il y a un léger abus ici puisque l'identité de $\Gamma(2)$ correspond au triplet trivial $(1, 0, 1)$.

Revenons-en aux triplets. Les quatre voisins du triplet $F(A)$ sont les sommets $F(U^{\pm 1}A)$ et $F(V^{\pm 1}A)$. Oubliant les contraintes de signe, rappelons-nous que $F(A) = (x, y, z)$, où :

$$\begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases} \quad \text{si } A = \begin{pmatrix} m & * \\ n & * \end{pmatrix} \in \tilde{\Gamma}(2).$$

Pour $\varepsilon = \pm 1$, on a : $F(U^\varepsilon A) = (x', y', z')$, où :

$$\begin{cases} x' = (m + 2\varepsilon n)^2 - n^2 = m^2 + 3n^2 + 4\varepsilon mn = -x + 2\varepsilon y + 2z \\ y' = 2(m + 2\varepsilon n)n = 2mn + 4\varepsilon n^2 = -2\varepsilon x + y + 2\varepsilon z \\ z' = (m + 2\varepsilon n)^2 + n^2 = m^2 + 5n^2 + 4\varepsilon mn = -2x + 2\varepsilon y + 3z. \end{cases}$$

Remplacer U par V revient à permuter formellement m et n, c'est-à-dire à remplacer x par $-x$. On résume le résultat.

3.17. Corollaire. *L'ensemble des triplets pythagoriciens primitifs est muni d'une structure d'arbre ternaire enraciné en* $(1, 0, 1)$. *Écrits en colonnes, les quatre voisins d'un triplet* $(x, y, z) \neq (1, 0, 1)$ *sont*[14] :

$$\begin{pmatrix} -x+2y+2z \\ -2x+y+2z \\ -2x+2y+3z \end{pmatrix}, \quad \begin{pmatrix} -x-2y+2z \\ 2x+y-2z \\ -2x-2y+3z \end{pmatrix}, \quad \begin{pmatrix} x+2y+2z \\ 2x+y+2z \\ 2x+2y+3z \end{pmatrix}, \quad \begin{pmatrix} x-2y+2z \\ -2x+y-2z \\ 2x-2y+3z \end{pmatrix}.$$

Références : Cette partie est une réinterprétation de l'article de Roger Alperin [1]. Elle donne une interprétation conceptuelle des résultats de l'article de Paul Préau [69]. Mais le premier auteur à ranger les triplets pythagoriciens le long d'un arbre aurait été J. F. M. Barning, vers 1963.

4. Birapport et configurations finies

Dans ce paragraphe, on prend pour $\mathbb{K}$ un corps fini $\mathbb{F}_q$ de caractéristique p. La droite projective contient alors $q + 1$ points. L'action de $\mathrm{PSL}_2(\mathbb{F}_q)$ sur $\mathbb{P}^1(\mathbb{F}_q)$ induit un morphisme $\mathrm{PSL}_2(\mathbb{F}_q) \to \mathfrak{S}_{q+1}$. Comme l'action est trois fois simplement transitive par [H2G2, §X-1.2.7], le morphisme est injectif. Pour les petites valeurs de q, on obtient par cardinalité (rappelons que $\mathrm{PSL}_2(\mathbb{F}_q)$ contient $q(q^2-1)/2$ éléments si $p > 2$ et $q(q^2-1)$ si $p = 2$ et que $\mathfrak{S}_n$ contient pour unique sous-groupe d'indice 2 le groupe alterné) :

- pour $q = 2$, un isomorphisme $\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$;
- pour $q = 3$, un isomorphisme $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$;
- pour $q = 4$, un isomorphisme $\mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$;

[14] En fait, on travaille ici aux signes de x, y, z près : pour être sûr d'avoir des triplets positifs, il faudrait mettre des valeurs absolues aussi disgracieuses qu'inutiles.

tout cela est contenu dans [H2G2, proposition VIII-3.1]. On a aussi relié $\mathrm{PSL}_2(\mathbb{F}_5)$ à $\mathfrak{A}_5$ dans le chapitre V. On étudie donc $\mathrm{PSL}_2(\mathbb{F}_7)$ dans ce chapitre. Voici un énoncé un peu ésotérique pour l'instant.

4.1. Théorème. *L'action de* $\mathrm{PSL}_2(\mathbb{F}_7)$ *sur les quatorze triangles équilatéraux de* $\mathbb{F}_7$ *admet deux orbites* T_1 *et* T_2 *de cardinal 7. Le plan de Fano se réalise comme une configuration dont les points (resp. les lignes) sont les triangles de* T_1 *(resp.* T_2*) et sur laquelle* $\mathrm{PSL}_2(\mathbb{F}_7)$ *agit (non trivialement).*

Ce théorème sera prouvé à la fin de cette partie. En attendant, on peut montrer qu'il a la conséquence suivante.

4.2. Corollaire. *Les groupes* $\mathrm{PSL}_2(\mathbb{F}_7)$ *et* $\mathrm{GL}_3(\mathbb{F}_2)$ *sont isomorphes.*

Démonstration. On sait par [3], 2.26, ou par l'exercice V-D.4, que le groupe des automorphismes de la configuration naturelle sur $\mathbb{P}^2(\mathbb{F}_2)$ est $\mathrm{GL}_3(\mathbb{F}_2)$.

Le groupe simple $\mathrm{PSL}_2(\mathbb{F}_7)$ agit fidèlement sur la configuration : il s'injecte dans $\mathrm{GL}_3(\mathbb{F}_2)$. On a d'une part $|\mathrm{PSL}_2(\mathbb{F}_7)| = (7^2-1)(7^2-7)/(2\times(7-1))$ et d'autre part $|\mathrm{GL}_3(\mathbb{F}_2)| = (2^3-1)(2^3-2)(2^3-2^2)$. L'égalité des cardinaux montre que l'injection est une isomorphisme. □

4.3. Parties équianharmoniques

L'ingrédient de base pour utiliser le birapport sur $\mathbb{F}_q$ est l'action de $\mathrm{PGL}_2(\mathbb{F}_q)$ sur les quadruplets de points de la droite projective $\mathbb{P}^1(\mathbb{F}_q)$. Mais il y en a trop : on regroupe alors les quadruplets par parties selon la valeur du birapport ; sauf que le birapport n'est pas invariant par permutation des variables (paragraphe 1), ce qui force à regrouper les quadruplets dont les birapports est dans une orbite de l'action de $\mathfrak{S}_3$ sur $\mathbb{P}^1(\mathbb{F}_q)$. Comme dans [H2G2, §X-1.2.22] sur les divisions harmoniques et équianharmoniques[15], on s'intéresse aux valeurs spéciales pour en avoir moins.

Supposons avoir $q \equiv 1 \pmod 3$: alors, $\mathbb{F}_q$ admet des racines primitives cubiques de 1, que l'on notera toujours j et j^2. Rappelons qu'une partie *équianharmonique* est une partie $\{z_1, z_2, z_3, z_4\}$ de $\mathbb{P}^1(\mathbb{F}_q)$ telle que $[z_1, z_2, z_3, z_4] \in \{-j, -j^2\}$.

4.4. Remarque ($q = 7$). Le corps $\mathbb{F}_7$ contient des racines primitives cubiques de l'unité : $j = 2$ et $j^2 = 4$. Avec les relations $4 = 1/2$, $3 = -j$ et $5 = -j^2$, on obtient :

$$\mathbb{P}^1(\mathbb{F}_7) = \{\infty, 0, 1\} \cup \{-1, 2, 1/2\} \cup \{-j, -j^2\}.$$

Ainsi, sur $\mathbb{F}_7$, un quadruplet est soit *harmonique* (si le birapport appartient à $\{-1, 2, 1/2\}$), soit équianharmonique (s'il se trouve dans $\{-j, -j^2\}$).

[15] Monique, Monique, cette incantation montre combien tu nous manques.

4.5. Lemme

(i) *Il existe vingt-huit parties équianharmoniques sur la droite projective* $\mathbb{P}^1(\mathbb{F}_7)$.

(ii) *L'action de* $\mathrm{PGL}_2(\mathbb{F}_7)$ *sur les parties équianharmoniques est transitive.*

(iii) *Le complémentaire d'une partie équianharmonique de* $\mathbb{P}^1(\mathbb{F}_7)$ *est une partie équianharmonique.*

(iv) *La droite projective* $\mathbb{P}^1(\mathbb{F}_7)$ *contient quatorze paires de parties équianharmoniques complémentaires.*

Démonstration. Soit $\mathbb{F}_q$ un corps fini de cardinal $q \equiv 1 \pmod 3$. D'après [H2G2, proposition X-1.2.7], pour un triplet d'éléments distincts (z_1, z_2, z_3) de $\mathbb{P}^1(\mathbb{F}_q)$, il y a exactement deux quadruplets ordonnés (z_1, z_2, z_3, z_4) tels que $[z_1, z_2, z_3, z_4] \in \{-j, -j^2\}$. Il y a donc $2(q+1)q(q-1)$ quadruplets ordonnés équianharmoniques. Comme ils sont tous formés de points distincts, il y a donc $(q+1)q(q-1)/12$ parties équianharmoniques dans $\mathbb{P}^1(\mathbb{F}_q)$. Pour $q = 7$, on en obtient : $8 \times 7 \times 6/12 = 28$.

Soit $\{z_1, z_2, z_3, z_4\}$ une partie équianharmonique. Soit h l'homographie qui envoie z_1 sur ∞, z_2 sur 0, z_3 sur 1. Par définition d'une partie équianharmonique, $h(z_4)$ vaut $-j = 3$ ou $-j^2 = 5$. Par suite, la partie $\{z_1, z_2, z_3, z_4\}$ est dans l'orbite de $\{\infty, 0, 1, 3\}$ ou $\{\infty, 0, 1, 5\}$. On en déduit la transitivité de l'action car l'inversion $z \mapsto 1/z$ permute ces deux parties.

Le complémentaire de la partie équianharmonique $\{\infty, 0, 1, 3\}$ est $\{2, 4, 5, 6\}$ et l'on a :

$$[2, 4, 5, 6] = \frac{2-5}{2-6} \times \frac{4-6}{4-5} = 5,$$

si bien que $\{2, 4, 5, 6\}$ est une partie équianharmonique. Par transitivité du groupe des homographies et invariance du birapport, le complémentaire de toute partie équianharmonique est encore équianharmonique.

La dernière assertion résulte de l'égalité : $28/2 = 14$. □

4.6. Définition. On appelle *triangle équilatéral de* $\mathbb{F}_7$ une partie à trois éléments $\{a, b, c\}$ de $\mathbb{F}_7$, notée abusivement (abc), telle que $\{\infty, a, b, c\}$ soit une partie équianharmonique de $\mathbb{P}^1(\mathbb{F}_7)$.

Cette dénomination charmante (pourtant peu répandue) vient du fait que pour un triplet $\{a, b, c\}$ de complexes, $[\infty, a, b, c] \in \{-j, -j^2\}$ si et seulement si abc est un triangle équilatéral. Cela donne une façon de paramétrer les paires de parties équianharmoniques complémentaires. Expliquons pourquoi et décrivons-les.

4.7. Lemme

(i) *L'application* $(abc) \mapsto \big\{\{\infty, a, b, c\}, \mathbb{P}^1 \setminus \{\infty, a, b, c\}\big\}$ *est une bijection entre triangles équilatéraux et paires de parties équianharmoniques complémentaires de* $\mathbb{P}^1(\mathbb{F}_7)$.

(ii) *Les triangles équilatéraux de* $\mathbb{F}_7$ *sont :*

$$(013),\ (124),\ (235),\ (346),\ (045),\ (156),\ (026),$$
$$(015),\ (126),\ (023),\ (134),\ (245),\ (356),\ (046).$$

Démonstration. Le point ∞ apparaît dans exactement une des deux parties d'une paire de parties équianharmoniques complémentaires, ce qui rend l'assertion (i) évidente.

(ii) Puisque $3 = -j$ et $5 = -j^2$, les parties $\{\infty, 0, 1, 3\}$ et $\{\infty, 0, 1, 5\}$ sont équianharmoniques. L'homographie $z \mapsto z + 1$ fixe ∞ et préserve le birapport : son action itérée permet de construire, à partir des deux premières, 14 parties équianharmoniques contenant ∞, et donc toutes parties équianharmoniques contenant ∞ par le lemme 4.5. Par passage au complémentaire, on obtient toutes les parties équianharmoniques, puis tous les triangles équilatéraux de $\mathbb{F}_7$. □

4.8. Lemme

(i) *Le stabilisateur dans* $\mathrm{PGL}_2(\mathbb{F}_7)$ *d'un triangle équilatéral est de cardinal* 24.

(ii) *Il est inclus dans* $\mathrm{PSL}_2(\mathbb{F}_7)$.

(iii) *L'action de* $\mathrm{PSL}_2(\mathbb{F}_7)$ *sur les triangles équilatéraux possède deux orbites de cardinal* 7 *: ce sont les lignes du lemme 4.7 (ii).*

Démonstration. (i) On a déjà vu que l'action de $\mathrm{PGL}_2(\mathbb{F}_7)$ sur les triangles équilatéraux est transitive. Comme il y a quatorze triangles, le stabilisateur K d'un triangle admet pour cardinal :

$$\frac{|\mathrm{PGL}_2(\mathbb{F}_7)|}{14} = \frac{(7^2-1)(7^2-7)}{6 \times 14} = \frac{48 \times 42}{6 \times 14} = 24.$$

(ii) Soit H le stabilisateur dans $\mathrm{PSL}_2(\mathbb{F}_7)$ du triangle (013), c'est-à-dire de la paire $\big\{\{\infty, 0, 1, 3\}, \{2, 4, 5, 6\}\big\}$. On remarque[16] tout d'abord que les homographies

$$h_1 : z \mapsto \frac{3}{z}, \quad h_2 : z \mapsto \frac{z+4}{z+6}, \quad h_3 : z \mapsto \frac{3z+4}{z+4}$$

s'identifient aux produits de transpositions

$$(\infty 0)(13)(25)(46), \quad (\infty 1)(03)(26)(45), \quad (\infty 3)(01)(24)(56).$$

Elles sont bien dans $\mathrm{PSL}_2(\mathbb{F}_7)$ et fixent le triangle (013), de même que l'involution $h_4 : z \mapsto \dfrac{2z+6}{z+5}$, qui permute $(\infty, 0, 1, 3)$ et $(2, 4, 6, 5)$.

[16] Ah ! L'intuition !

En fait, h_1 et h_3 sont deux involutions qui commutent : elles engendrent un groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ (on a : $h_2 = h_1 h_3$) et l'on a : $h_4 h_1 h_4 = h_3$. Aussi, h_1, h_3 et h_4 engendrent un groupe[17] de cardinal 8, produit semi-direct de $(\mathbb{Z}/2\mathbb{Z})^2$ par $\mathbb{Z}/2\mathbb{Z}$. En particulier, le cardinal de H est divisible par 8.

Enfin, poussé par l'intuition[18], on introduit l'homographie $h : z \mapsto 2z + 1$. Elle s'identifie au produit de 3-cycles (013)(254) et, comme 2 est un carré, c'est un élément de $\mathrm{PSL}_2(\mathbb{F}_7)$. Ainsi, le cardinal de H est divisible par 3.

Par le lemme chinois, le cardinal de H est divisible par 24. Mais, H est un sous-groupe du stabilisateur K dans $\mathrm{PGL}_2(\mathbb{F}_7)$, qui est d'ordre 24. Ainsi, H et K coïncident.

(iii) Le cardinal de l'orbite d'un triangle sous $\mathrm{PSL}_2(\mathbb{F}_7)$ est : $|\mathrm{PSL}_2(\mathbb{F}_7)|/24$, soit 7. Dans le lemme 4.7 (ii), tous les triangles ont été rangés par lignes en calculant l'orbite du premier triangle de la ligne par $z \mapsto z + 1$, qui est dans $\mathrm{PSL}_2(\mathbb{F}_7)$ donc les deux orbites sont bien les deux lignes. □

4.9. Remarque. L'indice du groupe engendré par h_1 et h_3 dans $\mathrm{PSL}_2(\mathbb{F}_7)$ est 42. Comme on sait, c'est "the Answer to the Ultimate Question of Life, the Universe and Everything". Cela semble toutefois être une coïncidence. Voir `http://www.math.ucr.edu/home/baez/42.html` pour une question motivée.

Une riche structure combinatoire...

Les triangles équilatéraux de $\mathbb{F}_7$ forment un ensemble de parties bien particulier :

(013), (124), (235), (346), (045), (156), (026),
(015), (126), (023), (134), (245), (356), (046).

Commençons par quelques « coïncidences » numériques. D'abord, chaque élément de $\mathbb{F}_7$ apparaît exactement dans six triangles, trois dans chaque orbite de $\mathrm{PSL}_2(\mathbb{F}_7)$ (une orbite est une ligne). Ensuite, chaque triangle possède exactement trois triangles adjacents, en appelant adjacents des triangles qui ont deux sommets communs ; les triangles adjacents sont dans l'autre ligne. On obtient ainsi une configuration de type $7_3 7_3$, au sens du chapitre V.

Mieux que ça : on peut, en s'autorisant un peu de redondance, dessiner les « triangles équilatéraux de $\mathbb{F}_7$ » comme... des triangles équilatéraux du plan,

[17] On peut remarquer que c'est un 2-Sylow de $\mathrm{PSL}_2(\mathbb{F}_7)$.

[18] Moins hypocritement, cette transformation apparaît en cherchant un élément d'ordre 3 dans $\mathrm{PSL}_2(\mathbb{F}_7)$, qui fixe ∞ (pour fixer les idées) et stabilise $\{\infty, 0, 1, 3\}$ et donc $\{2, 4, 5, 6\}$.

de sorte à en obtenir un pavage (figure 4.1) où l'adjacence combinatoire est bien l'adjacence du plan réel.

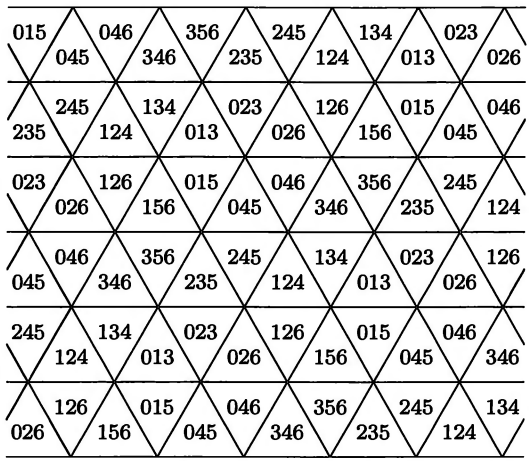


Figure 4.1. *Triangles équilatéraux de* $\mathbb{F}_7$

Dualement[19], dessinons le graphe d'incidence de cette configuration, dont les sommets sont les triangles, où il y a une arête entre deux triangles adjacents (figure 4.2 avec *seven shades of grey*).

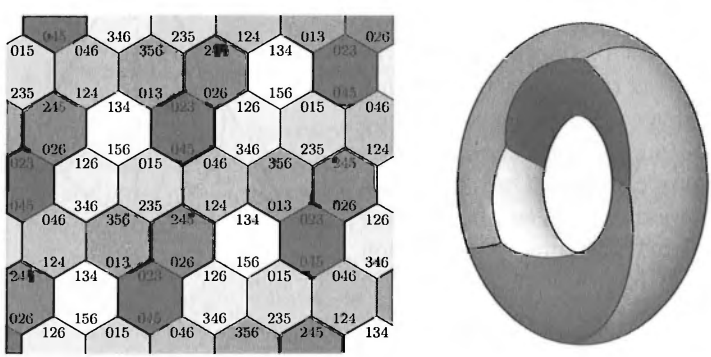


Figure 4.2. *Triangles équilatéraux de* $\mathbb{F}_7$*, versions duale et plongée*

Les deux graphes ont leurs sommets sur des réseaux d'indice 7 de $\mathbb{Z}^2$. Quotienter $\mathbb{R}^2$ par ce réseau plonge le graphe dans un tore, qu'il pave en faisant apparaître sept faces correspondant aux points de $\mathbb{F}_7$.

[19]Il s'agit de la dualité des graphes planaires, dans laquelle faces et sommets s'échangent. Deux faces adjacentes correspondent à deux sommets reliés par une arête dans le graphe dual.

4.10. Remarques. Le fait d'avoir un tore pavé[20] par des hexagones prouve que le nombre chromatique du tore est inférieur ou égal à 7, c'est-à-dire qu'il faut au moins sept couleurs pour être sûr de pouvoir colorier toute « carte » dessinée sur le tore ; dans ce registre, le célèbre « théorème des quatre couleurs » exprime que le nombre chromatique du plan est 4 ; de ce résultat difficile, on peut déduire que celui du tore est bien 7.

Par ailleurs, il existe des réalisations polyédrales des pavages du tore ci-dessus, dont on trouvera en ligne des patrons et des images animées plus convaincantes que ce que l'on pourrait dessiner ici :

- le *polyèdre de Szilassi* [81] possède sept faces hexagonales et quatorze sommets, chaque face a une arête commune avec les six autres ;
- le *polyèdre de Császár* possède quatorze faces triangulaires et sept sommets ; on peut le colorier avec deux couleurs, ce qui est un avatar de l'existence des deux orbites sous $\mathrm{PSL}_2(\mathbb{F}_7)$.

Mais une structure déjà connue : le plan de Fano

La dernière étape consiste à identifier les triangles équilatéraux au points du plan de Fano. Avec les triangles équilatéraux de $\mathbb{F}_7$, on construit la configuration suivante : les « points » de la configuration sont les triangles dans une des orbites sous $\mathrm{PSL}_2(\mathbb{F}_7)$; nommément, (013), (124), (235), (346), (045), (156), (026). Les « lignes » de la configuration sont les triangles de l'autre orbite : (015), (126), (023), (134), (245), (356), (046). La relation d'incidence est l'adjacence dans la figure 4.2 : deux triangles sont incidents s'ils ont deux points en commun. La configuration obtenue est représentée sur la figure ci-contre. On y reconnaît le plan de Fano. Mais en plus, elle est par construction munie d'une action non triviale du groupe $\mathrm{PSL}_2(\mathbb{F}_7)$. Cela prouve le théorème 4.1.

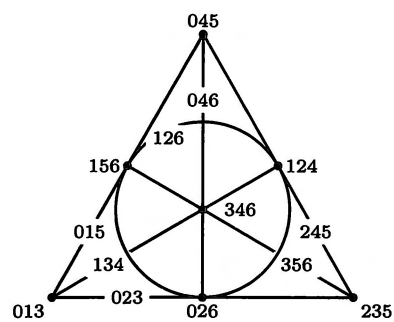


Figure 4.3. *Triangles équilatéraux de $\mathbb{F}_7$ et plan de Fano*

4.11. Remarque. Partant du plan de Fano, on forme son graphe d'incidence, qui est biparti : ses quatorze sommets sont les points et les lignes, il y a une arête entre un point et une ligne s'ils sont incidents. Par construction, on retrouve le graphe d'adjacence des triangles équilatéraux de $\mathbb{F}_7$.

Référence. Ce qui concerne la configuration $7_3 7_3$ apparaît déjà dans la référence [18, §4].

[20] De bonnes intentions ?

A. Annexe. Trajectoires orthogonales

Comme dans le corps du chapitre, on se place dans le demi-plan de Poincaré muni de la distance hyperbolique. On se donne une géodésique γ et une famille de géodésiques paramétrées par le même intervalle $[0,1]$, c'est-à-dire une famille de courbes $\gamma_s : [0,1] \to M$, où s décrit un voisinage de 0 dans $\mathbb{R}$ qui dépend de façon différentiable de s et telle que $\gamma_0 = \gamma$ et pour tout s, γ_s est une géodésique paramétrée par l'abscisse curviligne[21].

A.1. Proposition (Formule de la variation première de la longueur). *Avec les notations ci-dessus, on a :*

$$\left.\frac{\mathrm{d}L(\gamma_s)}{\mathrm{d}s}\right|_{s=0} = \langle V_1, T_1\rangle - \langle V_0, T_0\rangle,$$

où

$$V_0 = \gamma'(0) = \frac{\mathrm{d}\gamma_0}{\mathrm{d}t}(0) \quad \textit{et} \quad V_1 = \gamma'(1) = \frac{\mathrm{d}\gamma_0}{\mathrm{d}t}(1)$$

sont les vitesses de l'origine et de l'extrémité du segment mobile, et T_0, T_1 sont les vecteurs unitaires tangents au segment à l'origine et à l'extrémité.

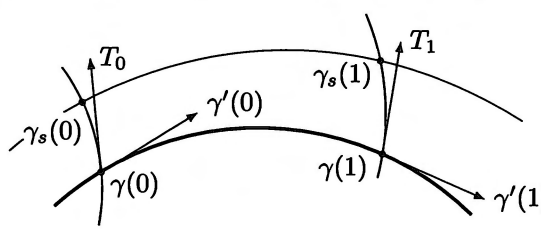


Figure A.1. *Variation de la longueur d'une géodésique $\gamma = \gamma_0$*

Ce théorème s'applique (beaucoup) plus généralement dans une variété M munie d'une métrique riemannienne g. Il faut alors utiliser g pour calculer le produit scalaire $\langle \cdot\,, \cdot \rangle$ entre vecteur normal et vecteur tangent. Sous cette forme étendue, c'est [11, théorème IX-80].

En fixant une extrémité, disons $\gamma_s(0) = m$ pour tout s, et en faisant varier $\gamma_s(1)$ sur un cercle hyperbolique, la longueur $L(\gamma_s)$ reste constante et la vitesse de l'origine V_0 s'annule, d'où : $\langle V_1, T_1\rangle = 0$.

A.2. Corollaire. *Soient m et n deux points du demi-plan de Poincaré. L'ensemble des points p tels que $d(m,p) = d(m,n)$ est une courbe dont la tangente en m est orthogonale à la géodésique qui relie m et n.*

L'énoncé plus général est appelé « lemme de Gauss » dans [32, théorème 2.93]. Nous remercions Pierre Pansu pour nous avoir indiqué ces résultats.

[21] C'est-à-dire que $\left\| \dfrac{\mathrm{d}\gamma_s(t)}{\mathrm{d}t} \right\| = 1$ pour tout t.

B. Exercices du chapitre VII

B.1. Exercice. *Suppose that u, v, z, w are complex numbers each a distance* 1 *from the point* 1 *in the complexe plane. Prove that if $uv = zw$ then $u = z$ or $u = w$.*

Hint: This is taxing if done directly. A useful quote from Wikipedia: "Many difficult problems in geometry become much more tractable when an inversion is applied." That is, try to characterize the reciprocals [inverses] of all points on the circle in the problem.

Cet exercice, échappé du tome premier, est tiré du numéro de juin 2014 du magazine Emissary, *édité par le Mathematical Research Institute de Berkeley.*

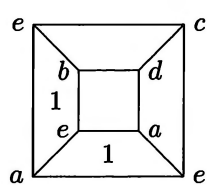
B.2. Exercice (Quintuplets de points à homographies près)

On a vu dans [H2G2, proposition X-1.2.13] que le birapport permet d'identifier l'ensemble des quadruplets de complexes deux à deux distincts à homographie près, que l'on a noté $(\mathbb{P}^1)^4_{\text{reg}}/\operatorname{PGL}_2(\mathbb{C})$, avec $X = \mathbb{P}^1(\mathbb{C})\setminus\{0,1,\infty\}$. On va trouver un analogue de X pour l'ensemble $(\mathbb{P}^1)^5_{\text{reg}}/\operatorname{PGL}_2(\mathbb{C})$, où $(\mathbb{P}^1)^5_{\text{reg}}$ est l'ensemble des quintuplets de points distincts, sur lequel $\operatorname{PGL}_2(\mathbb{C})$ agit de façon diagonale.

1. *Soit $(a,b,c,d,e) \in (\mathbb{P}^1)^5_{\text{reg}}$. Montrer la formule suivante :*

$$[a,b,d,e]\,[b,c,d,e]\,[c,a,d,e] = 1.$$

Par vérification directe ! C'est aussi une conséquence de la formule des six birapports avec $[e,e,a,c] = 1$, etc., en disposant les lettres comme suit :



2. *Soit $(a,b,c,d,e) \in (\mathbb{P}^1)^5_{\text{reg}}$. On pose $\bar{a} = [b,c,d,e]^{-1} \in \mathbb{P}^1$, $\bar{b} = [c,d,e,a]^{-1}$, et ainsi de suite par permutation circulaire, ce qui définit $\bar{c}$, $\bar{d}$ et $\bar{e}$. Montrer l'égalité $\bar{a}\,\bar{c} = 1 - \bar{b}$ et en déduire les relations analogues par permutation circulaire. Justifier que $\bar{b}\,\bar{d}$ ne vaut pas* 1.
Le produit $\bar{b}\,\bar{d}$ est le birapport $[a,e,b,d]$.
3. *On définit une application Ψ de l'ensemble $(\mathbb{P}^1)^5_{\text{reg}}$ des quintuplets de complexes deux à deux distincts dans $(\mathbb{P}^1)^2$, par $(a,b,c,d,e) \mapsto (\bar{b},\bar{d})$.*

Montrer que l'application Ψ passe au quotient par $\mathrm{PGL}_2(\mathbb{C})$, c'est-à-dire que deux quintuplets dans la même orbite ont la même image.

4. *Soit $(a,b,c,d,e) \in (\mathbb{P}^1)^5_{\mathrm{reg}}$. Montrer que l'on a :*

$$(\bar{a},\bar{b},\bar{c},\bar{d},\bar{e}) = \Big(\frac{1-\bar{b}}{1-\bar{b}\,\bar{d}}, \bar{b}, 1-\bar{b}\bar{d}, \bar{d}, \frac{1-\bar{d}}{1-\bar{b}\,\bar{d}}\Big).$$

5. *Soit (x,y) un élément de $X^2 \setminus \{(x,x^{-1}), x \in \mathbb{C}^*\}$. Montrer que l'image réciproque de (x^{-1},y^{-1}) par Ψ est l'orbite*

$$\mathrm{PGL}_2(\mathbb{C}) \cdot \Big(x, \frac{xy-1}{y-1}, \infty, 0, 1\Big).$$

6. *Conclure : identifier $(\mathbb{P}^1)^5_{\mathrm{reg}}/\mathrm{PGL}_2(\mathbb{C})$ et $X^2 \setminus \{(x,x^{-1}), x \in \mathbb{P}^1\}$.*

7. *Comme sous-produit de la construction, montrer que la fonction*

$$G : \mathbb{C}^2 \longrightarrow \mathbb{C}^2, \quad (s,t) \longmapsto \Big(t, \frac{1-s}{1-ts}\Big)$$

est d'ordre 5. Croyez-le ou pas, les amis : c'est encore un résultat de Gauss !

Si $(\bar{b},\bar{d}) = \Psi(\bar{a},\bar{b},\bar{c},\bar{d},\bar{e})$, alors $G(\bar{b},\bar{d}) = \Psi(\bar{c},\bar{d},\bar{e},\bar{a},\bar{b})$. (Le choix de $\bar{b}$ et $\bar{d}$ dans la définition de Ψ était arbitraire ; on peut par changement de variables (« de cartes ») permuter circulairement les coordonnées.)

8. *Construire une fonction H sur $\mathbb{C}^2$ qui correspond à l'inversion de l'ordre du quintuplet et en déduire une action du groupe diédral D_5 sur (un ouvert de) $\mathbb{C}^2$ par des fractions rationnelles.*

Si $(\bar{b},\bar{d}) = \Psi(\bar{a},\bar{b},\bar{c},\bar{d},\bar{e})$, on veut avoir : $H(\bar{b},\bar{d}) = \Psi(\bar{e},\bar{d},\bar{c},\bar{b},\bar{a})$. Pas dur.

Droites projectives de petit cardinal

B.3. Exercice (Isomorphismes exceptionnels de groupes finis et birapport)

Le but de l'exercice est de montrer comment le birapport permet d'exhiber certains morphismes exceptionnels. On notera z_1, z_2, z_3, z_4 quatre éléments de $\mathbb{P}^1(\mathbb{F}_q)$ deux à deux distincts.

1. $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ *: établir cela en faisant appel à la triple transitivité du groupe projectif sur la droite projective, [H2G2, proposition X-1.2.7].*

2. $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ *: constater que sur $\mathbb{P}^1(\mathbb{F}_3)$, il n'y a qu'un seul birapport possible pour $[z_1,z_2,z_3,z_4]$, à savoir -1 ; en déduire le résultat annoncé.*

Les valeurs 0, ∞ et 1 ne sont pas des birapports possibles, car les z_i sont deux à deux distincts.

3. $\mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$ *: montrer qu'il n'y a que deux birapports possibles pour* $[z_1, z_2, z_3, z_4]$ *et que* $[z_2, z_1, z_3, z_4] = [z_1, z_2, z_3, z_4]^{-1} \neq [z_1, z_2, z_3, z_4]$ *; en déduire que les deux groupes en question sont bien isomorphes.*

   La permutation σ est dans l'image de l'action si et seulement si $\sigma \cdot (12)$ n'y est pas.

B.4. Exercice (Conjugaison harmonique)

Soient Q et R deux points distincts de la droite projective sur un corps quelconque.

1. *Montrer que pour tout point P distinct de Q et R, il existe un unique P' tel que le birapport $[P, P', Q, R] = -1$. On dit que le point P' est le* conjugué harmonique *de P par Q et R.*

   On tombe sur une équation du premier degré...

2. *On prolonge la conjugaison harmonique en une homographie de la droite projective. Quels sont ses points fixes ?*

3. *Montrer que si P' est le conjugué harmonique de P par Q et R, alors :*

   (a) le point P est le conjugué harmonique de P' par Q et R ;

   (b) le point P' est le conjugué harmonique de P par R et Q ;

   (c) le point Q est le conjugué harmonique de R par P et P'.

   En particulier, la conjugaison harmonique est une involution.

4. *Montrer que si $P = \infty$, alors P' est le milieu (la moyenne) de Q et R.*

B.5. Exercice (Synthèmes harmoniques et isomorphisme $\mathbf{PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5}$).

La droite projective $\mathbb{P}^1(\mathbb{F}_5)$ permet de retrouver notre isomorphisme exceptionnel préféré[22] $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ *grâce au birapport.*

1. *Montrer que le birapport de quatre points deux à deux distincts de $\mathbb{P}^1(\mathbb{F}_5)$ est dans $\{-1, 2, 3\} = \{-1, 2, 1/2\}$.*

   On écrira $h(P_1, P_2; P_3, P_4)$ pour dire : $[P_1, P_2, P_3, P_4] = -1$.

2. *Montrer, en utilisant la proposition 1.3, que $h(P_1, P_2; P_3, P_4)$ implique $h(P_2, P_1; P_3, P_4)$, $h(P_1, P_2; P_4, P_3)$ et $h(P_3, P_4; P_1, P_2)$.*

   On dit que les paires $\{P_1, P_2\}$, $\{P_3, P_4\}$ sont *harmoniquement séparées* ; la question donne un sens à cette définition.

3. *On fixe deux points distincts P_1, P_2 de $\mathbb{P}^1(\mathbb{F}_5)$.*

   (a) Montrer que l'on peut ordonner les quatre points restants P_3, P_4,P_5 et P_6 de sorte à avoir $h(P_3, P_4; P_5, P_6)$.

[22] Non ?

(b) *Montrer qu'alors P_2 est le conjugué harmonique de P_1 par P_3 et P_4 (exercice B.4).*

Ce conjugué harmonique existe et est unique, ce n'est pas P_5 : sinon, P_1 serait le conjugué harmonique de P_5 par P_3 et P_4. Or, ce conjugué est P_6 par hypothèse. Par élimination, on finit par trouver que c'est P_2.

(c) *En déduire que les trois paires $\{P_1,P_2\}$, $\{P_3,P_4\}$, $\{P_5,P_6\}$ sont deux à deux harmoniquement séparées.*

On dit que la partition en paires $\big\{\{P_1,P_2\},\{P_3,P_4\},\{P_5,P_6\}\big\}$ est un *synthème harmonique.*

4. *Montrer qu'il existe cinq synthèmes harmoniques.*

Comme P_1, P_2 peuvent être pris quelconques distincts, on ne perd aucune généralité à prendre $P_1=\infty$, puis $P_2\in\mathbb{F}_5$.

5. *Montrer que $\mathrm{PGL}_2(\mathbb{F}_5)$ agit sur les 5 synthèmes harmoniques. En déduire l'isomorphisme : $\mathrm{PGL}_2(\mathbb{F}_5)\simeq\mathfrak{S}_5$.*

On montre, par la propriété du birapport, que l'action est bien définie, transitive et fidèle. L'isomorphisme s'obtient par cardinalité[23].

Pour information, les cinq synthèmes sont les suivants :

$$\big\{\{\infty,0\},\{1,-1\},\{2,-2\}\big\},\ \big\{\{\infty,1\},\{0,2\},\{-2,-1\}\big\},$$
$$\big\{\{\infty,2\},\{0,-1\},\{1,-2\}\big\},$$
$$\big\{\{\infty,-2\},\ \{0,1\},\{2,-1\}\big\},\ \big\{\{\infty,-1\},\{0,-2\},\{1,2\}\big\}.$$

B.6. Exercice (Triangles équilatéraux sur $\mathbb{F}_7$ et triangles autopolaires)

Dans l'exercice V-D.5, on a vu apparaître quatorze « triangles autopolaires spéciaux » dans la configuration du plan de Fano. Par le corollaire V-2.15, un triangle autopolaire s'identifie à un sous-groupe de $\mathrm{PSL}_2(\mathbb{F}_7)$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. On établit ici une correspondance naturelle avec les triangles équilatéraux de ce chapitre définis dans $\mathbb{P}^1(\mathbb{F}_7)$.

1. *Soit g un élément de $\mathrm{SL}_2(\mathbb{F}_7)$ dont l'image $[g]$ dans $\mathrm{PSL}_2(\mathbb{F}_7)$ est une involution. Montrer que g est conjugué à $g_1=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$.*

2. *Déterminer deux involutions $[g_2]$ et $[g_3]$ qui commutent avec $[g_1]$ et entre elles.*

Par le lemme V-2.14 (iii), il s'agit de trouver $g_2\in\mathrm{SL}_2(\mathbb{F}_7)$ tel que $\mathrm{tr}(g_1g_2)=0$. Cela donne deux paires d'involutions.

[23] Il est bien entendu qu'une fois que l'on sait que nos deux groupes sont isomorphes, on déduit facilement qu'il existe exactement 5! isomorphismes entre eux.

3. *On fait agir naturellement le groupe engendré par* $[g_1]$ *et* $[g_2]$ *sur* $\mathbb{P}^1(\mathbb{F}_7)$. *Déterminer les orbites de cette action et constater que ce sont deux paires de parties équianharmoniques complémentaires.*

   On trouve $\{\{\infty,0,2,3\},\{1,4,5,6\}\}$ ou $\{\{\infty,0,4,5\},\{1,2,3,6\}\}$.

4. *Établir une correspondance* $\mathrm{PGL}_2(\mathbb{F}_7)$*-équivariante entre triangles autopolaires et paires de parties équianharmoniques complémentaires.*

   Par le « principe de conjugaison », l'action de $\mathrm{PGL}_2(\mathbb{F}_7)$ par conjugaison sur les sous-groupes de $\mathrm{PSL}_2(\mathbb{F}_7)$ et l'action sur les orbites d'un tel sous-groupe dans $\mathbb{P}^1(\mathbb{F}_7)$ sont compatibles. Or, les actions sur les « triangles autopolaires » et sur les « triangles équilatéraux » sont transitives (proposition V-2.16 et lemme 4.7). Pour une approche plus terre-à-terre, on conjuguera le sous-groupe et la paire de parties équianharmoniques précédents par les homographies $z \mapsto z^{-1}$ (une fois) et $z \mapsto z+1$ (douze fois).

Pour résumer, on a des bijections naturelles entre les objets suivants : triangles du plan $\mathbb{P}\mathfrak{sl}_2(\mathbb{F}_7)$ *autopolaires par rapport à la conique nilpotente, sous-groupes de* $\mathrm{PSL}_2(\mathbb{F}_7)$ *isomorphes au groupe de Klein, paires de parties équianharmoniques complémentaires de* $\mathbb{P}^1(\mathbb{F}_7)$ *(*aka *triangles équilatéraux). Pour chaque type d'objets, on a de plus une relation d'adjacence naturelle permettant de définir une configuration isomorphe au plan de Fano, ce qui* in fine *explique l'isomorphisme exceptionnel* $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{PSL}_3(\mathbb{F}_2)$.

B.7. Exercice (Invariant d'homographies sur un corps fini et théorie de Galois). *Soit* $\mathbb{F}_q$ *un corps fini. On fait agir* $G = \mathrm{PGL}_2(\mathbb{F}_q)$ *sur le corps des fractions rationnelles* $\mathbb{F}_q(X)$ *par homographies (on vérifie que l'on a bien une action) en posant :*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot F(X) = F\Big(\frac{aX+b}{cX+d}\Big), \quad F \in \mathbb{F}_q(X).$$

Soit :

$$R = \frac{(X^{q^2}-X)^{q+1}}{(X^q-X)^{q^2+1}} \in \mathbb{F}_q(X).$$

On veut montrer que R *engendre le corps* $\mathbb{F}_q(X)^{\mathrm{PGL}_2(\mathbb{F}_q)}$ *des invariants.*

1. *En remarquant que* G *est engendré*[24] *par* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ *et* $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ $(a \in \mathbb{F}_q^*)$, *montrer que* $R \in \mathbb{F}_q(X)^G$.

[24] Cela résulte du fait que $\mathrm{GL}_n(\mathbb{K})$ est engendré par les dilatations et les transvections.

2. *Soient :*

$$P = \prod_{x \in \mathbb{F}_q^2 \setminus \mathbb{F}_q} (X - x) \quad et \quad Q = X^q - X.$$

Montrer que $P \in \mathbb{F}_q[X]$ *et que*

$$R = \frac{P^{q+1}}{Q^{q^2-q}}.$$

Le polynôme P est invariant par le Frobenius $F : x \mapsto x^q$, car ce dernier stabilise $\mathbb{F}_q^2 \setminus \mathbb{F}_q$. L'égalité vient de la relation

$$(X^{q^2} - X) = \prod_{x \in \mathbb{F}_q^2 \setminus \mathbb{F}_q} (X - x) \prod_{x \in \mathbb{F}_q} (X - x) = PQ.$$

3. *Montrer que le polynôme* $P^{q+1}(Y) - R(X)Q^{q^2-q}(Y)$ *s'annule en* $Y = X$ *et en déduire que le degré de* $\mathbb{F}_q(X)$ *sur* $\mathbb{F}_q(R)$ *est inférieur à* $q^3 - q$. *Conclure alors que* $\mathbb{F}_q(X)^G = \mathbb{F}_q(R)$.

On a une inclusion claire. Pour l'autre inclusion, on voit que le degré de $\mathbb{F}_q(X)$ sur $\mathbb{F}_q(X)^G$ est, par la théorie de Galois : $|G| = q^3 - q$.

The world has gotten even stranger than you already know.
Joss Whedon, *Avengers*, 2012.

Chapitre VIII

Encores sur les coniques

Ce chapitre propose deux historiettes sur les coniques en prise avec la grande histoire — théorème de Mordell, *geometric invariant theory*. Dans une première partie, partant de manipulations simples, voire simplettes en coordonnées, on munit les coniques d'une structure de groupe qui en fait une version dégénérée des courbes elliptiques. Puis, on revisite la classification euclidienne des coniques par la théorie des invariants : c'est peut-être une façon de motiver les approches algébriques de la géométrie.

1. Structure de groupe sur une conique

Dans cette partie, on munit les coniques les plus simples d'une structure de groupe. Puis, on constate que cette définition s'étend à n'importe quelle conique affine (modulo le choix d'un point). On en donne une application arithmétique à l'équation de Pell-Fermat. Puis, pour défrayer la conique, on interprète la construction dans un cadre projectif comme une dégénérescence d'une structure fascinante : les courbes elliptiques.

1.1. Les coniques affines réelles comme groupes

Soit $\mathscr{C}$ une conique affine sur un corps $\mathbb{K}$ de caractéristique différente de 2, et soit E un point de $\mathscr{C}$ (voué à devenir le neutre de la loi de groupe à venir). Étant donnés deux points A et B de $\mathscr{C}$, on définit un point $A * B$ de la façon suivante :

- soit Δ_{AB} la droite parallèle à la droite (AB) contenant E ; si $A = B$, on définit Δ_{AA} comme la parallèle à la tangente à $\mathscr{C}$ en A passant par E ;
- la droite Δ_{AB} coupe $\mathscr{C}$ en deux points, distincts ou pas : l'un des deux est E, l'autre est, par définition, $A * B$.

1.2. Proposition. *L'opération $*$ décrite ci-dessus est bien définie et munit $\mathscr{C}$ d'une structure de groupe abélien dont E est le neutre. À isomorphisme près, la structure ne dépend pas de E.*

Si la conique est définie sur $\mathbb{R}$ ou $\mathbb{C}$, c'est un groupe topologique.

La proposition sera démontrée au paragraphe 1.13. Pour l'heure, on va examiner quelques exemples sur le corps des réels.

L'hyperbole $xy = 1$. Dans le plan affine $\mathbb{R}^2$, notons x et y les coordonnées habituelles et considérons l'hyperbole $\mathscr{H}$ d'équation $xy = 1$; le point E est le point $(1,1)$. Soient $A = (a, 1/a)$ et $B = (b, 1/b)$ deux points de $\mathscr{H}$. Si a et b sont distincts, la droite Δ_{AB} a pour équation :

$$y - 1 = \frac{\frac{1}{b} - \frac{1}{a}}{b - a}(x - 1), \quad \text{ou encore : } y - 1 = -\frac{1}{ab}(x - 1).$$

Comme $\mathscr{H}$ est le graphe de la fonction $x \mapsto x^{-1}$, qui a pour dérivée $x \mapsto -x^{-2}$, cette dernière équation est aussi celle de Δ_{AA} lorsque $B = A$.

L'équation aux abscisses de l'intersection de $\mathscr{H}$ et Δ_{AB} est :

$$\frac{1 - x}{x} = -\frac{1}{ab}(x - 1),$$

qui admet pour solutions $x = 1$ et $x = ab$. Ainsi, les coordonnées du point $A * B$ sont $\big(ab, 1/(ab)\big)$.

Autrement dit, la loi $*$ sur $\mathscr{H}$ s'identifie à la multiplication sur $\mathbb{R}^*$ via la première projection $(a, a^{-1}) \mapsto a$.

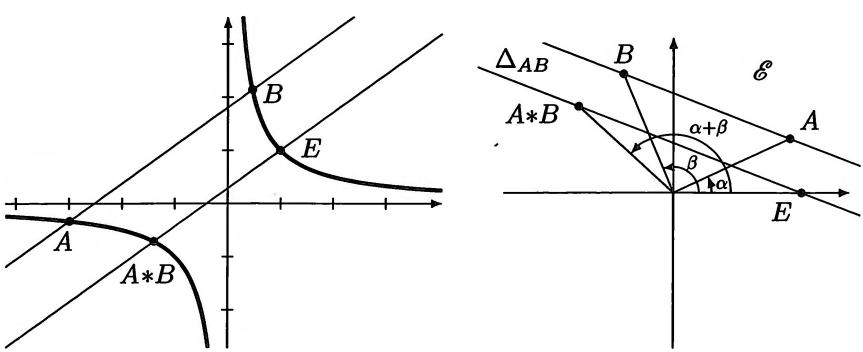


Figure 1.1. *Loi de groupe sur une hyperbole et sur un « cercle »*

Le « cercle-unité ». Dans le plan $\mathbb{R}^2$, considérons le cercle $\mathscr{C}$ d'équation $x^2 + y^2 = 1$ et $E = (1,0)$. Soient $A = (\cos\alpha, \sin\alpha)$ et $B = (\cos\beta, \sin\beta)$

deux points de $\mathscr{C}$, avec $\alpha, \beta \in \mathbb{R}/2\pi\mathbb{Z}$. On pourrait procéder comme ci-dessus, écrire et résoudre des équations, mais l'on va se laisser porter par l'optimisme ambiant. Prouvons donc que $A * B$ est le point :

$$C = \big(\cos(\alpha+\beta), \sin(\alpha+\beta)\big).$$

Pour ce faire, il suffit de prouver que la droite passant par E et le point C est parallèle à la droite (AB) (ou à la tangente en A si $B = A$). Si A et B sont distincts, la droite Δ_{AB} est dirigée par le vecteur

$$\begin{pmatrix}\cos\beta-\cos\alpha\\ \sin\beta-\sin\alpha\end{pmatrix} = 2\sin\frac{\beta-\alpha}{2}\begin{pmatrix}-\sin\dfrac{\alpha+\beta}{2}\\ \cos\dfrac{\alpha+\beta}{2}\end{pmatrix}, \text{ donc par } v = \begin{pmatrix}-\sin\dfrac{\alpha+\beta}{2}\\ \cos\dfrac{\alpha+\beta}{2}\end{pmatrix}.$$

La tangente à $\mathscr{C}$ en A est portée par le vecteur $(-\sin\alpha, \cos\alpha)$, si bien que le vecteur v ci-dessus dirige Δ_{AB}, même lorsque A et B sont égaux.

La droite Δ_{AB} est verticale si et seulement si $\sin(\alpha+\beta)/2 = 0$, ce qui revient à dire que α et β sont opposés dans $\mathbb{R}/2\pi\mathbb{Z}$. Alors, l'intersection de Δ_{AB} avec $\mathscr{C}$ est le point double E, si bien que $A * B = E = C$, comme annoncé.

Si, au contraire, on a : $\alpha+\beta \neq 0$, alors $\cos(\alpha+\beta) \neq 1$, si bien que $E \neq C$. Par suite, la droite (EC) a pour vecteur directeur

$$\begin{pmatrix}\cos(\alpha+\beta)-1\\ \sin(\alpha+\beta)\end{pmatrix} = 2\sin\frac{\alpha+\beta}{2}\begin{pmatrix}-\sin\dfrac{\alpha+\beta}{2}\\ \cos\dfrac{\alpha+\beta}{2}\end{pmatrix},$$

ce qui prouve que $\Delta_{AB} = (EC)$ et que $C = A * B$.

Autrement dit, la loi $*$ sur $\mathscr{C}$ s'identifie à l'addition sur $\mathbb{R}/2\pi\mathbb{Z}$ via le paramétrage $\alpha \mapsto (\cos\alpha, \sin\alpha)$.

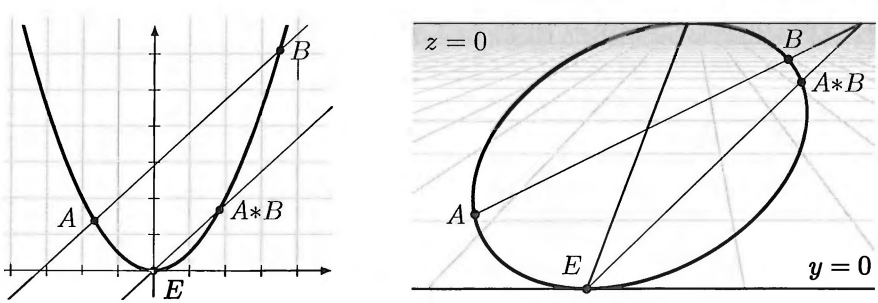


Figure 1.2. *Loi de groupe sur une parabole et vue en perspective*[1]

[1] À gauche, la conique est $\{y = x^2\}$. À droite, en coordonnées homogènes $[x : y : z]$, l'axe du bas est $\{y = 0\}$, l'horizon est $\{z = 0\}$, tous deux tangents à la conique $\{yz = x^2\}$.

La parabole $y = x^2$. Désignons par $\mathscr{P}$ la parabole d'équation $y = x^2$ et par E l'origine $(0,0)$. Des calculs analogues aux calculs précédents permettent d'établir que si $A = (a, a^2)$ et $B = (b, b^2)$ sont deux points de $\mathscr{P}$, on a alors : $A * B = \big(a+b, (a+b)^2\big)$.

Autrement dit, la loi $*$ sur $\mathscr{P}$ s'identifie à l'addition sur $\mathbb{R}$ via la première projection $(a, a^2) \mapsto a$.

Conique affine réelle quelconque. Soit $\mathscr{C}$ une conique affine réelle quelconque non dégénérée et soit E un point de $\mathscr{C}$. Par le théorème de classification, il existe des réels strictement positifs a, b et p et un repère affine dans lequel $\mathscr{C}$ a pour équation l'une des suivantes :

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} = 1, \quad \frac{X^2}{a^2} + \frac{Y^2}{b^2} = 1, \quad Y^2 = 2pX.$$

Vérifions qu'en faisant un changement de repère convenable, on retrouve l'une des trois équations traitées ci-dessus. Notons (X_E, Y_E) les coordonnées de E dans le repère précédent. Dans le cas d'une hyperbole, on pose :

$$\begin{cases} x = \dfrac{1}{k}\left(\dfrac{X}{a} + \dfrac{Y}{b}\right) \\ y = k\left(\dfrac{X}{a} - \dfrac{Y}{b}\right), \end{cases} \quad \text{où } k = \frac{X_E}{a} + \frac{Y_E}{b} = \frac{1}{\dfrac{X_E}{a} - \dfrac{Y_E}{b}}.$$

(On a alors : $X^2/a^2 - Y^2/b^2 = x^2 - y^2$.)

Pour une ellipse, on pose

$$\begin{cases} x = \dfrac{\cos\alpha_0}{a} X + \dfrac{\sin\alpha_0}{b} Y \\ y = -\dfrac{\sin\alpha_0}{a} X + \dfrac{\cos\alpha_0}{b} Y, \end{cases} \quad \text{où } \alpha_0 \text{ est choisi pour que } \begin{cases} \cos\alpha_0 = \dfrac{X_E}{a} \\ \sin\alpha_0 = \dfrac{Y_E}{b}. \end{cases}$$

(Si $X/a = \cos t$ et $Y/b = \sin t$, on a donc : $x = \cos(t - \alpha_0)$ et $y = \sin(t - \alpha_0)$. De plus, on a : $X^2/a^2 + Y^2/b^2 = x^2 + y^2$.)

Pour une parabole, on pose :

$$\begin{cases} x = 2p(X - X_E) - 2Y_E(Y - Y_E) = 2pX - 2Y_E Y + Y_E^2 \\ y = Y - Y_E, \end{cases} \quad \text{avec } Y_E^2 = 2pX_E.$$

(De la sorte, E est l'origine du nouveau repère et l'axe des y est la tangente à $\mathscr{P}$ en E ; qui plus est, on a : $x - y^2 = 2pX - Y^2$.)

Bilan provisoire

Les calculs précédents prouvent la proposition 1.2 sur le corps des réels. On identifie de plus le groupe obtenu selon le genre de la conique, indépendamment du choix de E. On voit ainsi apparaître tous les groupes que l'on sait paramétrer par un seul paramètre (c'est-à-dire de dimension 1).

1.3. Remarque. En fait, la classification des coniques sur un corps donné $\mathbb{K}$ constitue une classification des groupes algébriques affines de dimension 1. Grossièrement, les groupes algébriques affines sont des groupes qui sont le lieu des zéros d'une famille de polynômes dans un espace $\mathbb{K}^N$ et pour lesquels les coordonnées du produit de deux éléments et de l'inverse d'un élément sont des fractions rationnelles en les coordonnées des éléments. Des exemples de tels groupes sont $\mathbb{K}$, $\mathbb{K}^*$, $\mathrm{GL}_d(\mathbb{K})$, et désormais les coniques. Sur $\mathbb{R}$ ou $\mathbb{C}$, un groupe algébrique affine hérite d'une structure de groupe de Lie : c'est, si l'on veut, de cette notion de dimension dont il est question.

Une application à l'arithmétique

Le problème général est de trouver des *points rationnels* ou *entiers*, c'est-à-dire des points de $\mathbb{R}^2$ à coordonnées rationnelles ou entières, sur une conique définie par une équation à coefficients rationnels ou entiers. Dès que l'on connaît deux points rationnels sur une telle conique, disons M_0 et M_1, on peut en fabriquer d'autres par le procédé suivant. On note $*$ la structure de groupe sur la conique pour laquelle $E = M_0$. Alors, le sous-groupe engendré par M_1 est formé de points rationnels. En effet...

1.4. Lemme. *Soit $\mathscr{C}$ une* conique affine *non dégénérée ayant une équation à coefficients rationnels et soit E un point rationnel de $\mathscr{C}$. On note $*$ la structure de groupe sur $\mathscr{C}$ pour laquelle E est le neutre. Si A et B sont deux points rationnels de $\mathscr{C}$, alors le point $A * B$ en est un aussi.*

Démonstration. Si A et B sont deux points rationnels distincts, la droite Δ_{AB} admet un vecteur directeur rationnel. Il en est de même pour Δ_{AA}, puisque les coefficients de l'équation de $\mathscr{C}$ et les coordonnées de A sont rationnels. Comme l'intersection de Δ_{AB} et $\mathscr{C}$ contient un point rationnel E, l'autre est également rationnel. [En effet, paramétrons la droite Δ_{AB} sous la forme $x = at+b$, $y = ct+d$, avec a, b, c, d rationnels fixés et t paramètre rationnel. L'intersection est caractérisée par une équation à coefficients rationnels en t de degré au plus 2. En fait, le degré est exactement 2 : en effet, la partie quadratique de l'équation est la même que celle qui décrit l'intersection de $\mathscr{C}$ avec la droite (AB), qui a exactement deux solutions correspondant à A et B puisque $\mathscr{C}$ n'est pas dégénérée. Ainsi, cette équation en t, qui a une solution connue dans $\mathbb{Q}$, en a donc une deuxième dans $\mathbb{Q}$ puisque la somme des deux solutions est un rationnel.] □

Un exemple : l'équation de Pell-Fermat

L'*équation de Pell*, ou *équation de Pell-Fermat*, est une équation diophantienne quadratique : on cherche les couples d'entiers (x, y) solutions d'une équation de type $x^2 - dy^2 = e$, où d et e sont des entiers, avec d positif non carré.

1.5. Proposition. *Soit d un entier naturel sans facteur carré et soit $\mathscr{H}$ l'hyperbole ayant pour équation $X^2 - dY^2 = 1$ dans le plan $\mathbb{R}^2$. Soit $E = M_0 = (1,0)$. Soit $M_1 = (X_1, Y_1) \in \mathscr{H}$ avec X_1 et Y_1 entiers naturels non nuls et $X_1^2 + Y_1^2$ aussi petit que possible. Alors, l'ensemble des points entiers de la branche de $\mathscr{H}$ qui contient M_0 est le groupe engendré par M_1. L'ensemble des points entiers de $\mathscr{H}$ forme un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

1.6. Remarque. Le développement en fraction continue de $\sqrt{d}$ permet de trouver (X_1, Y_1), voir par exemple [24, théorème 4.6 et corollaire 4.3].

Démonstration. On calcule, en coordonnées, l'application $\mathscr{H} \to \mathscr{H}$, $M \mapsto M_1 * M$. Une façon de faire consiste à écrire et résoudre un système. Il est plus habile de passer du repère OXY à un repère Oxy dans lequel $\mathscr{H}$ a pour équation $xy = 1$ et M_0 a pour coordonnées $(1,1)$, en posant :

$$\begin{cases} x = X + \sqrt{d}Y \\ y = X - \sqrt{d}Y. \end{cases}$$

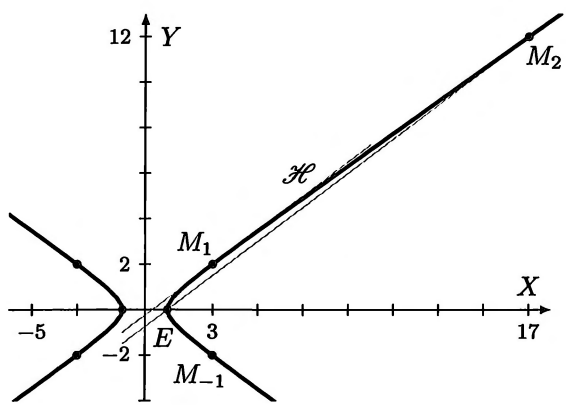


Figure 1.3. *Équation de Pell :* $x^2 - 2y^2 = 1$

Notons (x_1, y_1) les coordonnées de M_1 dans ce repère. Si un point M admet pour coordonnées (X, Y) dans un repère et (x, y) dans l'autre, $M_1 * M$ admet pour coordonnées $(x_1 x, y_1 y)$ dans ce dernier et l'on vérifie qu'il a pour coordonnées

$$M_1 * M = (X', Y') = (X_1 X + dY_1 Y, Y_1 X + X_1 Y)$$

dans le premier. Notons, pour référence ultérieure, la relation :

$$(\heartsuit) \qquad X' + \sqrt{d}Y' = (X_1 + \sqrt{d}Y_1)(X + \sqrt{d}Y).$$

L'hyperbole $\mathscr{H}$ est la réunion de deux branches (ses composantes connexes). Comme dans le repère Oxy, l'opération de groupe est le produit coordonnée par coordonnée, $\mathscr{H}$ est un groupe topologique. Par conséquent, la branche $\mathscr{H}_0$ contenue dans le demi-plan $X > 0$, en tant que composante neutre de $\mathscr{H}$, est un sous-groupe. La projection sur l'axe des x permet d'identifier $\mathscr{H}_0$ à $\mathbb{R}^{+*}$, ce qui donne un ordre sur $\mathscr{H}_0$. Si les coordonnées dans Oxy d'un point $M = (X, Y)$ de $\mathscr{H}_0$ sont (x, y), on a : $x = \sqrt{1 + dY^2} + \sqrt{d}Y$. Cette fonction de Y est strictement croissante, et l'ordre se lit donc indifféremment sur la coordonnée x ou sur la coordonnée Y. Par exemple, pour cet ordre, l'application $\varphi : \mathscr{H}_0 \to \mathscr{H}_0$, $M \mapsto M_1 * M$ est strictement croissante puisque les coordonnées dans Oxy de $\varphi(M)$ sont $(x_1 x, y_1 y)$ et que $x \mapsto x_1 x$ est strictement croissante.

Pour $n \in \mathbb{Z}$, notons $M_n = M_1^n = (X_n, Y_n)$. On vérifie que $M_{-1} = M_1^{-1} = (X_1, -Y_1)$, d'où l'on déduit par récurrence que $Y_{-n} = -Y_n$ pour tout n. Comme φ est strictement croissante et que $M_{n+1} = \varphi(M_n)$, la suite $(M_n)_{n\in\mathbb{Z}}$ est strictement croissante. De plus, comme $X_1 \geqslant 1$, $Y_1 > 0$ et $X_n \geqslant 1$ pour tout n, on a : $Y_{n+1} > Y_n$ pour tout $n \in \mathbb{Z}$. Comme tous les Y_n sont entiers, Y_n tend vers l'infini lorsque n tend vers l'infini.

Mais alors, soit $M = (X, Y)$ un point de $\mathscr{H}_0$. D'après le paragraphe précédent, il existe n naturel tel que $Y_n \leqslant Y < Y_{n+1}$. Notons $M' = (X', Y') = M_{-n} * M$. Grâce à la croissance stricte de φ, donc de φ^{-n}, on a : $M_0 \leqslant M' < M_1$. Mais, par hypothèse, M_1 est la solution entière *minimale* de l'équation de Pell, ce qui entraîne : $M' = M_0$ puis $M = M_n$.

On remarque à présent que la réflexion $\sigma : (X, Y) \mapsto (-X, Y)$ échange les deux branches de $\mathscr{H}$ et préserve $\mathbb{Z}^2$, et l'on peut affirmer que les points entiers de $\mathscr{H}$ sont de la forme $(\pm X_n, Y_n)$ pour $n \in \mathbb{Z}$. En fait, σ est le produit $M \mapsto F * M$, où $F = (-1, 0) \in \mathscr{H}$. La proposition en découle. □

1.7. Un anneau, ses inversibles et sa norme

Tout ceci s'interprète dans l'anneau[2] $A = \mathbb{Z}[\sqrt{d}]$. L'ensemble des solutions de l'équation de Pell est en bijection avec les éléments de A de norme 1, où la norme de $X + \sqrt{d}Y$ est

$$N\big(X + \sqrt{d}Y\big) = X^2 - dY^2.$$

Il n'y a pas loin pour aller jusqu'à décrire tous les inversibles de A : en effet, un élément $X + \sqrt{d}Y$ est inversible si et seulement si sa norme est inversible, c'est-à-dire si et seulement si $M = (X, Y)$ est un point entier de

[2] L'anneau A est à peu de choses près l'anneau $\mathscr{O}$ des entiers algébriques de $\mathbb{Q}(\sqrt{d})$. Plus précisément, $\mathscr{O}$ est $\mathbb{Z}[(1 + \sqrt{d})/2]$ si $d \equiv 1 \pmod 4$ et $\mathbb{Z}[\sqrt{d}]$ sinon.

l'une des deux hyperboles :

$$X^2 - dY^2 = \pm 1.$$

Vu la formule (♡), l'identification $(X, Y) \mapsto X + \sqrt{d}Y$ qui, à un point entier de $\mathscr{H}$ associe un inversible de norme 1, est un isomorphisme de groupes. D'après la proposition, le noyau de la norme est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Il peut arriver que l'hyperbole $X^2 - dY^2 = -1$ n'ait pas de point entier –par exemple, si $d = 7$, puisque -1 n'est pas un carré modulo 7. Dans ce cas, $A^\times = \ker N$. Mais, supposons qu'il y en ait un, c'est-à-dire qu'il y ait dans A un élément $\tilde{a} = \tilde{X} + \sqrt{d}\tilde{Y}$ de norme -1. Alors tout élément de norme -1 est le produit de $\tilde{a}$ par un élément de norme 1, c'est-à-dire que l'on a :

$$A^\times = \ker(N) \cup \tilde{a} \ker(N) \simeq \mathbb{Z}/2\mathbb{Z} \times \ker N.$$

Au bilan, on a décrit les inversibles de $A = \mathbb{Z}[\sqrt{d}]$:

$$A^\times \simeq \mathbb{Z} \times \Gamma, \quad \text{où } \Gamma \simeq \mathbb{Z}/2\mathbb{Z} \text{ ou } (\mathbb{Z}/2\mathbb{Z})^2.$$

On retrouve ainsi, dans le cas le plus facile, le « théorème des unités » des anneaux d'entiers algébriques, voir [71, §4.4, théorème 1] : comme $\mathbb{Q}(\sqrt{d})$ possède un seul plongement dans $\mathbb{C}$ et que ce plongement est réel, $A^\times$ est le produit de $\mathbb{Z}$ par un groupe fini.

1.8. Vision projective : une courbe elliptique dégénérée

Restons provisoirement sur les réels, mais plongeons dans le plan projectif et tâchons d'y comprendre la loi $*$. Par une homographie du plan projectif bien choisie, on peut envoyer n'importe quelle conique non dégénérée sur n'importe quelle autre. Comme une homographie préserve l'alignement, l'incidence et la tangence[3], il suffit de traduire la notion affine de parallélisme en la notion projective correspondante bien connue : deux droites affines sont parallèles si et seulement si, quand on les plonge dans le plan projectif, elles se coupent sur la droite à l'infini, voir par exemple [H2G2, figure XI-2.3].

Construction de la loi $*$ sur $\mathscr{C} \setminus \mathscr{D}$. On se donne donc, dans un plan projectif quelconque, sur un corps quelconque $\mathbb{K}$ de caractéristique différente de 2, une conique projective non dégénérée $\mathscr{C}$, une droite $\mathscr{D}$ que nous appellerons « droite à l'infini » et un point E de $\mathscr{C}$ qui n'est pas sur $\mathscr{D}$. Étant donnés deux points A et B de $\mathscr{C} \setminus \mathscr{D}$, on note p_{AB} l'intersection de $\mathscr{D}$ avec la

[3]Pour la tangence, voici deux arguments. Dans un ouvert affine du plan projectif, les coordonnées de l'image par une homographie sont des fractions rationnelles en les coordonnées du point, donc elles sont différentiables partout où elles sont définies. Pour une conique, la droite tangente en un point $[x : y : z]$ de $\mathbb{P}^2(\mathbb{R})$ est l'image d'un plan de $\mathbb{R}^3$, le plan orthogonal à (x, y, z) pour la forme quadratique qui définit la conique : cette situation est préservée par une application linéaire.

droite (AB) (ou la tangente à $\mathscr{C}$ en A si $A = B$), puis l'on considère la droite Δ_{AB} qui passe par E et p_{AB} (ou la tangente à $\mathscr{C}$ en E si $p_{AB} = E$). La droite Δ_{AB} coupe $\mathscr{C}$ en deux points, distincts ou confondus (d'après le lemme suivant), E et $A * B$.

1.9. Lemme. *Soit $\mathbb{K}$ un corps de caractéristique différente de 2, soit Q une forme quadratique non dégénérée sur $\mathbb{K}^3$ et soit $\mathscr{C}$ la conique projective d'équation $Q = 0$ dans $\mathbb{P}^2(\mathbb{K})$. Soit enfin $\mathscr{D}$ une droite projective de $\mathbb{P}^2(\mathbb{K})$. Alors :*

(i) *si $\mathbb{K}$ est algébriquement clos, l'intersection de $\mathscr{C}$ et $\mathscr{D}$ est la réunion de deux points éventuellement confondus ;*

(ii) *si $\mathbb{K}$ n'est pas algébriquement clos, l'intersection est soit vide, soit constituée de deux points, qui sont confondus si et seulement si $\mathscr{D}$ est tangente à $\mathscr{C}$.*

Démonstration. La droite $\mathscr{D}$ est la projection dans $\mathbb{P}^2(\mathbb{K})$ d'un plan vectoriel Π de $\mathbb{K}^3$. Comme Q est non dégénérée, l'orthogonal de Π est une droite, si bien que le noyau de la restriction de Q à Π est de dimension au plus 1. Autrement dit, la restriction de Q à Π n'est pas nulle. On peut trouver une base de Π, dont on note (x_1, x_2) la base duale et que l'on complète en une base (x_1, x_2, x_3) du dual de $\mathbb{K}^3$, dans laquelle $Q|_\Pi$ est de la forme $\alpha_1 x_1^2 + \alpha_2 x_2^2$, avec $(\alpha_1, \alpha_2) \in \mathbb{K}^* \times \mathbb{K}$ (voir [H2G2, proposition V-B.3.1]).

(i) Supposons $\mathbb{K}$ algébriquement clos. Alors, en coordonnées homogènes dans la base précédente, l'intersection $\mathscr{C} \cap \mathscr{D}$ est le point double $[0 : 1 : 0]$ ou les points $\left[\sqrt{-\alpha_2} : \pm\sqrt{\alpha_1} : 0\right]$, selon que α_2 est nul ou pas.

(ii) Pour $\mathbb{K}$ quelconque, on voit que si l'un des deux points $\left[\sqrt{-\alpha_2} : \pm\sqrt{\alpha_1} : 0\right]$ (qui sont *a priori* définis dans $\mathbb{P}^2(\overline{\mathbb{K}})$) appartient à $\mathbb{P}^2(\mathbb{K})$ alors l'autre point aussi. En effet, l'intersection d'une droite avec une conique donne lieu à une équation de degré inférieur à 2 à coefficient dans $\mathbb{K}$. Le cas algébriquement clos montre que cette équation est bien de degré 2, puisqu'il y a deux solutions, ou une double. Et, comme la somme des racines d'une équation du second degré sur $\mathbb{K}$ est dans le corps $\mathbb{K}$, on déduit qu'il y a, soit aucune intersection, soit deux, distinctes ou confondues. □

La proposition 1.2 est équivalente à la suivante.

1.10. Proposition. *La loi $*$ définie ci-dessus fait de $\mathscr{C} \setminus \mathscr{D}$ un groupe abélien.*

Démonstration. La loi $*$ est bien définie par le lemme 1.9. On vérifie également au passage que l'on reste bien dans $\mathscr{C} \setminus \mathscr{D}$.

La commutativité de la loi $*$ va de soi puisque les droites Δ_{AB} et Δ_{BA} sont égales pour tout couple de points (A, B). Le point E est neutre pour $*$. En

effet, pour tout point A, la droite Δ_{AE} est la droite (AE) elle-même (ou la tangente à $\mathscr{C}$ en E si $A = E$), si bien que $A * E = A$.

Tout point admet un symétrique pour $*$. En effet, soit E' l'intersection de la tangent à $\mathscr{C}$ en E avec la droite $\mathscr{D}$. Pour tout point A de $\mathscr{C}$, soit A' la deuxième intersection de $\mathscr{C}$ avec la droite (AE') (ou A si (AE') est tangente à $\mathscr{C}$ en A). Alors, $\Delta_{AA'}$ est la tangente à $\mathscr{C}$ en E, d'où : $A * A' = E$.

L'associativité fait l'objet du paragraphe 1.13. □

1.11. Remarque. Si $\mathbb{K} = \mathbb{R}$, on retrouve trois groupes ($\mathbb{R}^*$, $\mathbb{R}$ ou $\mathbb{R}/2\pi\mathbb{Z}$) correspondant aux trois genres de coniques selon que la droite $\mathscr{D}$ coupe $\mathscr{C}$ en deux, un ou zéro points, exactement comme dans la figure 20 (p. 251) de [4]. Si $\mathbb{K} = \mathbb{C}$, en revanche, $\mathscr{C}$ coupe $\mathscr{D}$: pas d'ellipse sur les complexes, et deux groupes obtenus de cette façon : $\mathbb{C}^*$ et $\mathbb{C}$.

1.12. Remarque. La donnée d'une droite et d'une conique projective est équivalente à celle d'un polynôme *factorisable* de degré 3, le produit de leurs équations (à une constante multiplicative près). Si l'on se donne à la place une courbe $\mathscr{E}$ dont l'équation est un polynôme homogène *irréductible* de degré 3, on tombe exactement sur la définition de l'addition sur la *courbe elliptique*[4] $\mathscr{E}$, pour peu que l'on reformule légèrement la définition de $*$. Il faut définir p_{AB} comme le troisième point d'intersection de la droite (AB) avec $\mathscr{E}$ et $A * B$ comme le troisième point d'intersection de Δ_{AB} avec $\mathscr{E}$. Pour être sûr de toujours avoir une tangente lorsque deux points coïncident, A et B ou p_{AB} et E, on doit supposer que $\mathscr{E}$ est lisse. Sur le corps des complexes, il est fascinant de relier cette construction à l'addition sur $\mathbb{C}/\Lambda$, où Λ est un réseau de $\mathbb{C}$, grâce à la fonction $\wp$, voir la remarque VII-1.8 ou mieux, le paragraphe VI-2 de [5], en particulier VI-2.5 et VI-2.6, ainsi que les exercices VI-9 à VI-12.

Dans cet esprit, tout en gardant toute la modestie nécessaire, on peut voir la recherche des points entiers sur l'hyperbole en utilisant la loi de groupe de façon géométrique comme une version faible, dégénérée au même sens que ci-dessus et incomparablement plus simple, du théorème de Mordell, qui affirme que le groupe des points rationnels d'une courbe elliptique est de type fini.

On retiendra (ou pas) que la loi de groupe sur une conique est la trace de la loi de groupe sur une courbe elliptique lorsque celle-ci dégénère en la réunion d'une conique et d'une droite.

On peut enfin remarquer que la même règle fonctionne si l'on prend A sur $\mathscr{C} \setminus \mathscr{D}$ et B sur $\mathscr{D} \setminus \mathscr{C}$. Dans ces conditions, p_{AB} est le deuxième point d'intersection de $\mathscr{C}$ et de (AB) (le « premier » est A...) et $A * B$ est le troisième

[4]Pour une définition simple mais non canonique, une courbe elliptique est une courbe projective plane lisse ayant une équation de la forme $Y^2Z = 4X^3 + g_2XZ^2 + g_3Z^3$ dans un repère idoine.

point d'intersection de $\mathscr{C} \cup \mathscr{D}$ avec (Ep_{AB}) (les deux « premiers », E et p_{AB} sont sur $\mathscr{C}$) : il appartient à $\mathscr{D}$, ce qui définit une action de notre groupe $\mathscr{C} \setminus \mathscr{D}$ sur $\mathscr{D} \setminus \mathscr{C}$.

1.13. Théorème de Pascal et associativité

On garde les hypothèses de 1.8. On va montrer l'associativité de la loi $*$. L'idée frappante, pour la moitié au moins des auteurs, c'est que l'associativité est essentiellement équivalente au *théorème de l'hexagramme mystique de Pascal* (voir [4, théorème VII-4.4]).

Rappelons le théorème, ou plutôt un prolongement « par continuité » de celui-ci où certains points de l'hexagramme peuvent être confondus. On convient que pour deux points A et B de la conique $\mathscr{C}$, on note (AB) la droite passant par A et B si $A \neq B$ et la tangente à la conique en A si $A = B$.

1.14. Théorème. *On considère une conique projective non dégénérée $\mathscr{C}$ sur $\mathbb{K}$ et six points A, B, C, A', B', C' sur la conique. Soient X, Y et Z les intersections respectives de (AB') et $(A'B)$, de (AC') et $(A'C)$ et de (BC') et $(B'C)$ — on suppose que les deux droites de chaque paire sont distinctes. Alors, les points X, Y et Z sont alignés.*

B.U. PRODUIT DE L'ANNÉE

Revenons à l'associativité. Soient trois points A, B et C sur $\mathscr{C} \setminus \mathscr{D}$.

Pour commencer, on suppose les points A et C distincts. On veut montrer que $(A * B) * C = A * (B * C)$. Pour cela, il suffit de montrer que les droites $\Delta_{A,B*C}$ et $\Delta_{A*B,C}$ sont confondues, ce qui résultera de l'égalité $p_{A,B*C} = p_{A*B,C}$. Notons q l'intersection des droites $(A, B * C)$ et $(A * B, C)$: il suffit de montrer que q appartient à $\mathscr{D}$ (figure 1.4), on aura bien : $q = p_{A,B*C} = p_{A*B,C}$.

Notons que les points p_{AB} et p_{BC} sont distincts. En effet, s'ils étaient confondus, un coup d'œil sur la figure et une pensée pour le lemme 1.9 nous donneraient que A et C sont confondus, contrairement aux hypothèses.

D'après le *théorème de Pascal*, les points p_{AB}, p_{BC} et q sont alignés. Comme p_{AB} et p_{BC} appartiennent à $\mathscr{D}$, et comme ils sont distincts, la droite (p_{AB}, p_{BC}) est la droite $\mathscr{D}$; on peut donc affirmer que q appartient aussi à $\mathscr{D}$, ce qui termine la preuve dans ce cas.

Supposons $A = C$. Si de plus $A = B$, il n'y a rien à montrer. Sinon, la commutativité implique l'égalité voulue, car on a : $A*(B*A) = A*(A*B) = (A * B) * A$.

Références : Ce thème fait l'objet de nombreux problèmes de concours. On le trouve également dans [41, exercice V-5.6].

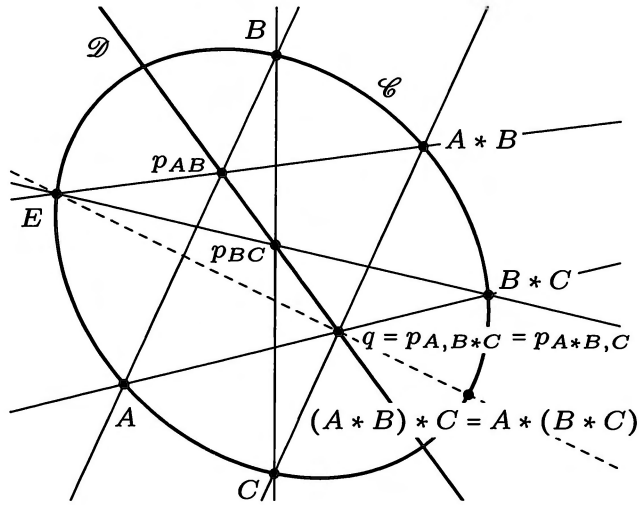


Figure 1.4. *Associativité de* $*$

2. Coniques et théorie des invariants

Cette partie est inspirée de l'exemple introductif de [61]. On veut comprendre la classification des coniques à isométrie près d'un point de vue « dual » de celui du tome premier, et « algébrique », comme dans « géométrie algébrique ». L'outil est la théorie des invariants, c'est-à-dire l'étude des fonctions polynomiales sur l'espace **E** des équations des coniques qui sont invariantes par l'action du groupe des isométries du plan (réel ou complexe, au choix).

2.1. Position du problème

Soit **F** l'espace des fonctions polynomiales sur $\mathbb{C}^2$. Pour étudier les coniques, on s'intéresse à l'espace **E** des « équations de coniques », c'est-à-dire le sous-espace de **F** formé des polynômes de degré inférieur ou égal à 2 en deux variables x, y, c'est-à-dire de la forme

$$F(x,y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f.$$

Par [H2G2, lemme V-6.3], qui identifie polynômes formels et fonctions polynomiales, la famille $(x^2, 2xy, y^2, 2x, 2y, 1)$ est une base de **E**. Ainsi, **E** est un espace de dimension 6 muni de coordonnées notées encore (a,b,c,d,e,f), qui forment dans $\mathbf{E}^*$ la base duale de $(x^2, 2xy, y^2, 2x, 2y, 1)$.

Poussé par la philosophie de la géométrie algébrique, « étudier l'algèbre des fonctions pour étudier la géométrie », on forme l'algèbre des polynômes à valeurs complexes *sur* l'espace **E**, autrement dit les polynômes *en* les

coordonnées $a, b, \dots, f$, c'est-à-dire l'algèbre de polynômes :

$$\mathbf{P} = \mathbb{C}[a, b, c, d, e, f].$$

Ou plutôt ses invariants par un groupe. Soit G un sous-groupe du groupe affine du plan, par exemple le groupe des isométries ou des similitudes affines. Il agit sur le $\mathbb{C}$-espace $\mathbf{F}$: si $F \in \mathbf{F}$ et $g \in \tilde{G}$, on pose :

$$\forall (x, y) \in \mathbb{R}^2, \quad (g \cdot F)(x, y) = F\big(g^{-1} \cdot (x, y)\big).$$

C'est une action linéaire de G sur $\mathbf{F}$. Comme l'action de G sur le plan est affine, si F est un polynôme en x et y, alors $g \cdot F$ est un polynôme de même degré. Cela signifie que $\mathbf{E}$ est stable sous l'action de G. En dualisant l'action, on obtient une action sur l'espace $\mathbf{E}^*$ engendré par $a, b, \dots, f$: pour $\ell \in \mathbf{E}^*$ et $g \in G$, on définit $g \cdot \ell$ par son image en $F \in \mathbf{E}$:

$$(g \cdot \ell)(F) = \ell(g^{-1} \cdot F) = \ell\Big(F\big(g(x, y)\big)\Big).$$

Pour $\ell = a$ par exemple, $g \cdot a$ est le coefficient de x^2 dans $F\big(g(x, y)\big)$, en posant $F = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f$. On donnera des formules au lemme 2.5.

De même que l'on est passé ci-dessus d'une action sur le plan à une action sur les polynômes en x, y, l'action linéaire de G sur l'espace engendré par $a, b, \dots, f$ induit une action sur $\mathbf{P}$ par automorphismes d'algèbres — c'est une conséquence de la propriété universelle des algèbres de polynômes, voir l'annexe A.

Une « fonction polynomiale » sur le quotient de notre espace par G devrait être une fonction polynomiale P sur l'espace qui prend la même valeur sur chaque orbite, c'est-à-dire invariante par tout élément $g \in G$: $g \cdot P = P$. On va donc calculer la sous-algèbre des invariants $\mathbf{P}^G$ avec l'idée que cette algèbre pourrait tenir lieu d'algèbre de fonctions sur l'ensemble des orbites de coniques sous l'action de G (exercice B.2).

2.2. Remarque. Homogénéisons comme dans [H2G2, §V-6.2 et §V-6.3]. L'action de $g \in G$ sur un élément (x, y) est de la forme :

$$g \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ux + u'y + x_0 \\ vx + v'y + y_0 \end{pmatrix} = R_g \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \quad \text{où } R_g = \begin{pmatrix} u & u' & x_0 \\ v & v' & y_0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On peut calculer $F(x, y)$ par :

$$F(x, y) = \begin{pmatrix} x & y & 1 \end{pmatrix} A_F \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \quad \text{où } A_F = \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}.$$

Ainsi, $g \cdot F$ est déterminé par la matrice ${}^t R_g A_F R_g$.

2.3. Exemple. L'action de la symétrie, $(x,y)\mapsto(x,-y)$, d'axe Ox parallèlement à Oy, sur $\mathbb{C}^6$ donne l'automorphisme $(a,b,c,d,e,f)\mapsto(a,-b,c,d,-e,f)$.

2.4. Exemple. Regardons l'action de la translation, $(x,y)\mapsto(x+x_0,y+y_0)$ de vecteur (x_0,y_0) sur $\mathbb{C}^6$. On trouve l'automorphisme

$$(a,b,c,d,e,f)\mapsto(a,b,c,x_0a+y_0b+d,x_0b+y_0c+e,\\ x_0^2a+2x_0y_0b+y_0^2c+2x_0d+2y_0e+f).$$

2.5. Lemme. *Soit g un élément de G donné par la matrice R_g ci-dessus. L'action de g sur $\mathbf{E}^*$ est décrite par sa matrice dans la base (a,b,c,d,e,f) :*

$$\begin{pmatrix} u^2 & uu' & u'^2 & ux_0 & u'x_0 & x_0^2 \\ 2uv & uv'+vu' & 2u'v' & uy_0+vx_0 & u'y_0+v'x_0 & 2x_0y_0 \\ v^2 & vv' & v'^2 & vy_0 & v'y_0 & y_0^2 \\ 0 & 0 & 0 & u & u' & 2x_0 \\ 0 & 0 & 0 & v & v' & 2y_0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Démonstration. Soit $F(x,y)=ax^2+2bxy+cy^2+2dx+2ey+f$, où toutes les lettres sont des indéterminées. Il s'agit tout simplement de développer

$$F\big(g(x,y)\big)=F(ux+u'y+x_0,vx+v'y+y_0),$$

et de séparer les coefficients. Par exemple, le coefficient d de $2x$ est :

$$ux_0a+(uy_0+vx_0)b+vy_0c+ud+ve,$$

ce qui détermine la quatrième colonne de la matrice. Détails omis. □

2.6. Remarques. On ne manipulera ces formules que dans des cas particuliers : rotations centrées en l'origine et translations.

Sur l'expression générale, on peut remarquer que le sous-espace engendré par a,b,c et celui engendré par $a,\dots,e$ sont stables par G : c'est synonyme de la conservation du degré des polynômes en x,y. Toutefois, ils ne possèdent pas de supplémentaire stable (sauf si l'on se restreint au stabilisateur de l'origine dans G).

2.7. Notations. Jusqu'à la fin de cette partie, on note G le groupe des isométries affines du plan et $\tilde{G}$ le groupe des similitudes affines du plan. Un élément de G (resp. de $\tilde{G}$) est de la forme

$$g:\begin{pmatrix}x\\y\end{pmatrix}\mapsto\begin{pmatrix}ux-\varepsilon vy+x_0\\vx+\varepsilon uy+y_0\end{pmatrix},$$

où $\varepsilon=\pm1$ et u, v, x_0 et y_0 sont des scalaires tels que $u^2+v^2=1$ (resp. $u^2+v^2\neq0$).

Les éléments qui fixent l'origine, *i.e.* tels que $x_0 = y_0 = 0$, forment un sous-groupe isomorphe à $\mathrm{O}_2(\mathbb{R})$. Parmi eux, pour θ réel, on notera g_θ la rotation correspondant à $u = \cos\theta$, $v = \sin\theta$, $\varepsilon = 1$, $x_0 = y_0 = 0$. Les g_θ forment un sous-groupe isomorphe à $\mathrm{SO}_2(\mathbb{R})$. Les matrices telles que $u = 1$, $v = 0$ forment le sous-groupe normal G_0 des translations. On a : $G \simeq G_0 \ltimes \mathrm{SO}_2(\mathbb{R})$.

Enfin, on pose :

$$D = \det A_F = \det \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} \in \mathbf{P} = \mathbb{C}[a, b, c, d, e, f].$$

2.8. Lemme. *Le polynôme D est invariant par G, c'est-à-dire : $D \in \mathbf{P}^G$.*

Démonstration. Cela provient de la description matricielle de l'action. Soit $g \in G$. Alors, $g \cdot D$ est le déterminant de la matrice associée à $g \cdot F$, c'est-à-dire ${}^t R_g A_F R_g$. Or, comme g, la matrice R_g a pour déterminant ± 1, de sorte que le déterminant D est invariant. □

2.9. Proposition. *Les invariants de l'action de $\mathrm{SO}_2(\mathbb{R})$ et $\mathrm{O}_2(\mathbb{R})$ sur $\mathbb{C}[a, b, c]$ sont :*

$$\mathbb{C}[a, b, c]^{\mathrm{SO}_2(\mathbb{R})} = \mathbb{C}[a, b, c]^{\mathrm{O}_2(\mathbb{R})} = \mathbb{C}[T, E], \quad \text{où } \begin{cases} T = a + c, \\ E = ac - b^2. \end{cases}$$

Démonstration. La preuve utilise implicitement la (très simple) théorie des représentations de $\mathrm{SO}_2(\mathbb{R})$. Le sous-espace vectoriel $V = \mathbb{C}a \oplus \mathbb{C}b \oplus \mathbb{C}c$ est stable par $\mathrm{SO}_2(\mathbb{R})$. D'après le lemme 2.5, la matrice de g_θ dans la base (a, b, c) est :

$$\begin{pmatrix} \cos^2\theta & -\cos\theta\sin\theta & \sin^2\theta \\ 2\cos\theta\sin\theta & \cos^2\theta - \sin^2\theta & -2\cos\theta\sin\theta \\ \sin^2\theta & \cos\theta\sin\theta & \cos^2\theta \end{pmatrix}.$$

Les vecteurs propres communs à tous les éléments g_θ ($\theta \in \mathbb{R}$) : $T = a + c$ (valeur propre 1), $R = a - c + 2ib$ (valeur propre $e^{2i\theta}$) et $S = a - c - 2ib$ (valeur propre $e^{-2i\theta}$). Ces trois vecteurs forment une base de V, et sont donc algébriquement indépendants et engendrent $\mathbb{C}[a, b, c]$ comme algèbre : $\mathbb{C}[a, b, c] = \mathbb{C}[R, S, T]$. Autrement dit, les monômes en R, S et T forment une base de $\mathbb{C}[a, b, c]$.

Comme $\mathrm{SO}_2(\mathbb{R})$ agit par automorphismes d'algèbres, les monômes en R, S et T sont des vecteurs propres des g_θ ; plus précisément, un monôme $R^r S^s T^t$ a pour valeur propre $e^{2i(r-s)\theta}$. En particulier, il est invariant si et seulement si l'on a : $r = s$. Ainsi, les polynômes invariants sont les

polynômes en T et

$$RS = (a-c)^2 + 4b^2 = (a+c)^2 - 4(ac-b^2) = T^2 - 4E,$$

c'est-à-dire que ce sont les polynômes en T et E.

Passons au groupe $\mathrm{O}_2(\mathbb{R})$. On observe que T et E sont invariants sous $\mathrm{O}_2(\mathbb{R})$ entier. En effet, l'action de $g \in \mathrm{O}_2(\mathbb{R})$ sur a, b et c se résume par :

$$g \cdot \begin{pmatrix} a & b \\ b & c \end{pmatrix} = {}^t g \begin{pmatrix} a & b \\ b & c \end{pmatrix} g = g^{-1} \begin{pmatrix} a & b \\ b & c \end{pmatrix} g\,;$$

pour le voir, extraire le bloc supérieur gauche de $A_{g\cdot F} = {}^t R_g A_F R_g$. Alors, T et E, qui sont la trace et le déterminant de cette matrice, sont invariants. Cela donne l'inclusion $\mathbb{C}[a,b,c]^{\mathrm{SO}_2(\mathbb{R})} \subset \mathbb{C}[a,b,c]^{\mathrm{O}_2(\mathbb{R})}$, l'inclusion inverse étant évidente. □

2.10. Remarque. Ce résultat ne devrait pas surprendre ! En effet, l'orbite d'une forme quadratique sous le groupe (spécial) orthogonal est déterminée par le spectre d'une matrice symétrique 2×2, lequel est déterminé par la somme T et le produit E des valeurs propres, qui sont la trace et le déterminant de la matrice.

2.11. Proposition (Invariants du groupe des isométries affines). *Les invariants de l'action de G sur $\mathbb{C}[a,b,c,d,e,f]$ sont :*

$$\mathbb{C}[a,b,c,d,e,f]^G = \mathbb{C}[T,E,D],$$

où

$$T = a + c, \quad E = ac - b^2, \quad D = \det \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}.$$

Démonstration (*tirée de [61]*). Bien sûr, T, E et D sont invariants, d'où l'inclusion de $\mathbb{C}[T,E,D]$ dans les invariants. Reste à voir l'inclusion inverse.

Soit G_0 le groupe des translations. Supposons savoir que l'on a :

$$\mathbb{C}[a,b,c,d,e,f]^{G_0} = \mathbb{C}[a,b,c,D].$$

Rappelons que G_0 est distingué dans G et que le quotient est le groupe orthogonal ; de plus, G stabilise l'espace engendré par a, b et c et l'action est celle que l'on connaît bien. Alors, grâce au lemme 2.9 et au fait que D est invariant, un polynôme en a, b, c et D qui est G-invariant est un polynôme en T, E et D, ce qui permet de conclure.

Montrons donc l'égalité annoncée. Pour cela, on plonge dans l'anneau[5] $\widehat{\mathbf{P}} = \mathbb{C}[a,b,c,d,e,f,1/E]$, qui possède toujours une action[6] de G. Vu que l'on a :

$$D = Ef + (2bde - ae^2 - cd^2),$$

on a dans $\widehat{\mathbf{P}}$:

$$f = \frac{D - 2bde + ae^2 + cd^2}{E},$$

d'où l'on déduit :

$$\mathbb{C}\Big[a,b,c,d,e,f,\frac{1}{E}\Big] = \mathbb{C}\Big[a,b,c,d,e,D,\frac{1}{E}\Big].$$

Pour terminer, il suffit de vérifier qu'un polynôme $P(a,b,c,d,e,D,1/E)$ invariant par translation n'a pas de terme en d et e. Pour cela, on écrit la relation d'invariance ($u = 1$, $v = 0$, $u' = 0$, $v' = 1$ dans le lemme 2.5 ou vérification directe) : pour tous $x_0, y_0 \in \mathbb{R}$,

$$P\Big(a,b,c,d,e,D,\frac{1}{E}\Big) = P\Big(a,b,c,d + x_0a + y_0b, e + x_0b + y_0c, D, \frac{1}{E}\Big).$$

En dérivant par rapport à x_0 et à y_0 et en prenant $x_0 = y_0 = 0$, il vient :

$$\begin{cases} a\dfrac{\partial P}{\partial d} + b\dfrac{\partial P}{\partial e} = 0 \\ b\dfrac{\partial P}{\partial d} + c\dfrac{\partial P}{\partial e} = 0, \end{cases} \quad \text{d'où} \quad \begin{cases} (ac - b^2)\dfrac{\partial P}{\partial d} = 0 \\ (ac - b^2)\dfrac{\partial P}{\partial e} = 0. \end{cases}$$

Par intégrité (en fait, on a même rendu $E = ac - b^2$ inversible en passant dans $\widehat{\mathbf{P}}$), on en déduit que P ne dépend ni de d, ni de e. □

2.12. Remarques. D'abord, le résultat est plausible en termes de dimensions : l'espace des équations de coniques est de dimension 6 (avec pour coordonnées $a,\dots,f$) et le groupe des isométries est de dimension 3 : il est naturel que le quotient soit décrit par une algèbre de dimension $6 - 3 = 3$.

D'autre part, l'anneau $\mathbb{C}[a,b,c,d,e,f,1/E]$ est naturellement l'anneau des fonctions « polynomiales » sur l'ouvert des formes telles que $E \neq 0$. Le passage par cet anneau consistait moralement à se restreindre à la partie dense des coniques à centre.

---

[5] Pour éviter la théorie de la localisation, on peut le définir comme l'anneau engendré par $a,\dots,f$ et $1/E$ dans le corps des fractions rationnelles en $a,\dots,f$.

[6] Pour $g \in G$, $F \in \mathbf{P}$ et $k \in \mathbb{N}$, on pose : $g \cdot (F/E^k) = (g \cdot F)/E^k$. Cela a un sens parce que E est invariant.

2.13. Interprétation

Fixons un triplet de scalaires (T, E, D), disons, avec $E \neq 0$. Le couple (T, E) permet de trouver deux scalaires (λ_1, λ_2) tels que

$$\lambda_1 + \lambda_2 = T \text{ et } \lambda_1 \lambda_2 = E,$$

donc de former une équation :

$$\lambda_1 x^2 + \lambda_2 y^2 + \frac{D}{E} = 0,$$

qui a les mêmes invariants T, E et D. Ce que l'on retrouve là est essentiellement l'équation réduite d'une conique, qui ne dépend que de l'orbite sous les isométries.

Retrouver ainsi des résultats géométriques (ici, la classification des coniques à isométrie près) par des méthodes purement algébriques n'est généralement pas gratuit, voire impossible. Ici, on a de la chance que le quotient puisse être muni d'une structure de variété algébrique (décrite par l'algèbre de polynômes $\mathbb{C}[T, E, D]$) ; une telle chance est rare, car en général on n'a pas assez de polynômes invariants pour définir un quotient intéressant (exercice B.2). Dans des situations plus générales, la « théorie géométrique des invariants »[7] consiste notamment à trouver des procédés de construction pour définir de « bons » quotients en géométrie algébrique.

2.14. Excentricité

On rappelle que l'on peut définir les coniques réelles à l'aide d'une directrice $\mathscr{D}$ et d'un foyer F, comme le lieu des points M tels que $MF = e\, d(M, \mathscr{D})$, où e désigne l'excentricité. L'excentricité apparaît comme un invariant pour l'action du groupe des similitudes sur les coniques. Nous allons voir un autre point de vue assez amusant sur l'excentricité. Ici, on travaille sur $\mathbb{R}$.

Lemme. *L'excentricité*[8] e *de la conique réelle déterminée par* T, E, *et* $D \neq 0$ *est solution de l'équation :*

$$e^2 - 1 + \frac{1}{e^2 - 1} = 2 - \frac{T^2}{E}.$$

(Par convention, $e = 1$ *si et seulement si* $E = 0$.*)*

Démonstration. Vu l'équation, on peut supposer que la conique est une conique à centre. Comme T, D et E sont invariants par isométries, on peut

[7] GIT pour les intimes, pour *geometric invariant theory*. Son développement doit beaucoup à David Mumford, mathématicien américain né en 1937, lauréat de la médaille Fields en 1974 pour ses travaux en géométrie algébrique.

[8] Malgré le conflit de notation sur e, on ne voit guère comment appeler autrement l'excentricité.

supposer que la conique est réduite, *i.e.* qu'elle a une équation de la forme :

$$\frac{x^2}{\alpha^2} + \varepsilon \frac{y^2}{\beta^2} = 1,$$

où $\alpha, \beta > 0$, $\varepsilon = \pm 1$. Pour une ellipse, *i.e.* si $\varepsilon = 1$, on suppose que $\alpha \geqslant \beta$ pour assurer que les foyers sont sur l'axe des x. Soient $\gamma > 0$, $F = (\gamma, 0)$, $\delta \in \mathbb{R}$ et $\mathscr{D}$ la droite d'équation $x = \delta$. Soient $M = (x, y)$ un point quelconque de la conique et $H = (\delta, y)$ le projeté orthogonal de M sur $\mathscr{D}$, on a :

$$\begin{cases} MF^2 = (x-\gamma)^2 + y^2 = \left(1 + \dfrac{\beta^2}{\alpha^2}\right)x^2 - 2\gamma x - \beta^2 + \gamma^2, \\ MH^2 = x^2 - 2\delta x + \delta^2. \end{cases}$$

Tous calculs faits, on trouve que l'équation $MF^2 = e^2 MH^2$ est satisfaite pour tout point M de la conique si et seulement si l'on a :

$$e^2 = 1 - \varepsilon \frac{\beta^2}{\alpha^2}, \quad \gamma = e\alpha, \quad \delta = \frac{\alpha}{e}.$$

Reste à vérifier l'équation sur e. On a d'une part :

$$e^2 - 1 + \frac{1}{e^2 - 1} = \frac{\beta^2}{\alpha^2} + \frac{\alpha^2}{\beta^2},$$

et d'autre part, comme $T = 1/\alpha^2 + \varepsilon/\beta^2$ et $E = \varepsilon/\alpha^2\beta^2$:

$$\frac{T^2}{2E} = \frac{\varepsilon\alpha^2\beta^2}{2}\left(\frac{1}{\alpha^4} + \frac{2\varepsilon}{\alpha^2\beta^2} + \frac{1}{\beta^4}\right) = \frac{\varepsilon}{2}\left(\frac{\beta^2}{\alpha^2} + \frac{\alpha^2}{\beta^2}\right) + 1. \qquad \square$$

Le lemme signifie que l'excentricité n'est pas une fonction polynomiale en T, E et D; cependant, c'est une solution d'une équation algébrique sur $\mathbb{C}[T, E, E^{-1}]$.

Il y a une petite surprise. Comme $T = \lambda_1 + \lambda_2$ et $E = \lambda_1\lambda_2$ pour λ_1 et λ_2 réels convenables supposés non nuls, on a, par l'inégalité arithmético-géométrique : $|T^2/E| \geqslant 2$. Mais, observons le graphe de la fonction $e \mapsto e^2 - 1 + 1/(e^2 - 1)$ sur $\mathbb{R}^+$.

Lorsque $E > 0$, on a $2 - T^2/E \leqslant -2$, et tout va bien : il y a exactement une solution $e \in [0, 1[$. Mais, pour $E < 0$, on a *deux* valeurs possibles pour l'excentricité, toutes deux supérieures à 1 ! C'est en fait normal (eh !), si l'on tient compte de D : en effet, T et E ne déterminent que la partie quadratique de l'équation de la conique, D détermine laquelle des deux solutions e il faut choisir. Plus précisément, T et $E < 0$ étant donnés, ceux-ci déterminent les deux valeurs propres de signes contraires λ_1 et λ_2, ce qui

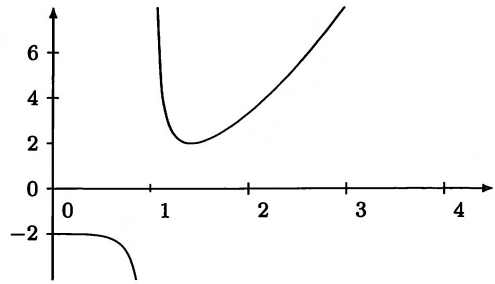


Figure 2.1. *L'équation* $e^2 - 1 + \dfrac{1}{e^2-1} = 2 - \dfrac{T^2}{E}$

donne l'équation réduite : $\lambda_1 x^2 + \lambda_2 y^2 + D/E = 0$. Selon le signe de D/E, on a deux façons d'apparier $\{|\lambda_1|, |\lambda_2|\}$ et $\{1/\alpha^2, 1/\beta^2\}$, d'où deux classes de similitude d'hyperboles dont les excentricités e et e' sont solutions de $e^2 = 1 + |\lambda_1/\lambda_2|$ et $e'^2 = 1 + |\lambda_2/\lambda_1|$ — autrement dit, $e'^2 - 1 = 1/(e^2-1)$; on remarque que la fonction $e \mapsto \big(1 + 1/(e^2-1)\big)^{1/2}$ est une involution de $]1, +\infty[$ dans lui-même.

Notons pour terminer sur le thème qu'en variables complexes, e est une fonction méromorphe multi-valuée de T, E et D.

A. Annexe. Polynômes sur, polynômes en...

Il est bien connu qu'une application linéaire sur un espace vectoriel V est une combinaison linéaire des coordonnées, *i.e.* des éléments d'une base de V^*. Dans cette annexe, on étend cette idée aux polynômes : une fonction polynomiale sur V est un polynôme en les coordonnées.

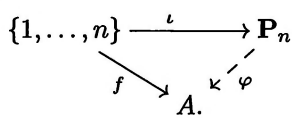
Ici, toutes les algèbres sont associatives, commutatives et unitaires et les morphismes préservent ces propriétés.

A.1. Algèbres de polynômes

Soit $\mathbb{K}$ un corps, soit n un entier naturel et soient $x_1, \dots, x_n$ des indéterminées — c'est-à-dire des symboles distincts et rien de plus. La définition naïve de l'algèbre de polynômes $\mathbb{K}[x_1, \dots, x_n]$ consiste à mettre une structure de produit sur l'ensemble des familles (a_α) indexées par $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ qui sont presque nulles, au sens où a_α est nul sauf pour un nombre fini d'indices α. On introduit alors des symboles $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ et l'on écrit $\sum_\alpha a_\alpha x^\alpha$ au lieu de (a_α).

On ne voit pas encore ce que l'on pourrait faire avec ça. La réponse est donnée par le *problème universel* suivant.

A.2. Proposition. *Soient $\mathbb{K}$ un corps et n un entier naturel. Il existe une algèbre $\mathbf{P}_n$ et une application $\iota : \{1, \dots, n\} \to \mathbf{P}_n$ telle que pour toute $\mathbb{K}$-algèbre A et toute application $f : \{1, \dots, n\} \to A$, il existe un unique morphisme d'algèbres $\varphi : \mathbf{P}_n \to A$ qui prolonge ι, c'est-à-dire qui fait commuter le diagramme*



On ne fait pas la démonstration, qui consiste essentiellement à montrer que l'algèbre $\mathbb{K}[x_1, \dots, x_n]$ convient pour $\mathbf{P}_n$. On a alors : $x_k = \iota(k)$ pour tout k ; de plus, $(x^\alpha)_{\alpha \in \mathbb{N}^n}$ est une base de $\mathbf{P}_n$. Si $A = \mathbb{K}$, le morphisme φ est l'évaluation au point $\big(f(1), \dots, f(n)\big)$. On gagne une clause d'unicité.

A.3. Corollaire. *Le couple $(\mathbf{P}_n, \iota)$ est unique à isomorphisme (unique) près.*

Le corollaire signifie que si $(\mathbf{P}', \iota')$ est une autre solution, alors le morphisme (unique) $\varphi : \mathbf{P}_n \to \mathbf{P}'$ déterminé par l'application $f = \iota' : \{1, \dots, n\} \to \mathbf{P}_n$ et le morphisme $\varphi' : \mathbf{P}' \to \mathbf{P}_n$ déterminé par $\iota : \{1, \dots, n\} \to \mathbf{P}_n$ sont des isomorphismes réciproques l'un de l'autre. C'est une conséquence de l'unicité dans la proposition.

Donnons-nous un espace vectoriel V de dimension finie sur $\mathbb{K}$. Soit $(e_1, \dots, e_n)$ une base de V, on note abusivement[9] $(x_1, \dots, x_n)$ la base duale. Comme (x^α) est une base de $\mathbf{P}_n$, la famille $(x_1, \dots, x_n)$ de $\mathbf{P}_n$ est libre, donc l'application $V^* \to \mathbf{P}_n$ qui envoie l'abusif x_k sur le x_k de $\mathbf{P}_n$ pour tout k est injective. L'abus était véniel, mais surtout, on peut considérer les éléments de $\mathbf{P}_n$ comme des polynômes en les éléments de V^*.

L'utilité de la chose est de voir V^*, engendré comme on le sait par les x_k, comme le sous-espace des polynômes homogènes de degré 1 dans $\mathbf{P}_n$. L'espace V^* est donc « prolongé » en une algèbre de polynômes. D'une part, on voit par l'unicité dans le corollaire, que cette algèbre ne dépend pas, à isomorphisme près, de la base choisie. D'autre part, on peut prolonger l'évaluation linéaire sur V en une évaluation polynomiale sur V. En effet, soit v fixé dans V. Pour ℓ dans V^*, soit φ l'application associée par la proposition à $f : \{1, \dots, n\} \to \mathbb{K}$, $k \mapsto x_k(v)$. Il est légitime d'appeler φ l'évaluation en v et l'on a, pour ℓ dans V^* : $\varphi(\ell) = \ell(v)$.

A.4. Définition. Posons $E = V^*$. Dans la construction précédente, l'algèbre $\mathbf{P}_n$ est appelée *algèbre des fonctions polynomiales sur* V et notée $\mathscr{S}(V^*) = \mathscr{S}(E)$. En ce sens, les polynômes *sur* V sont les polynômes *en* V^*.

Toute base $(x_1, \dots, x_n)$ de V^* donne une base de l'algèbre des fonctions polynomiales sur V : les monômes $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ avec $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. Nous allons voir maintenant que toute action linéaire sur V^* se prolonge en une *action par automorphismes* sur l'algèbre $\mathscr{S}(V^*)$.

A.5. Corollaire. *Soit u un élément du groupe linéaire de $V^* = \bigoplus_{k=1}^n \mathbb{K}x_k$. Il existe un unique automorphisme φ_u de $\mathscr{S}(V^*) = \mathbb{K}[x_1, \dots, x_n]$ tel que $\varphi_u|_{V^*} = u$. En particulier, on a*

$$\varphi_u\big(x_1^{\alpha_1} \cdots x_n^{\alpha_n}\big) = \varphi_u(x_1)^{\alpha_1} \cdots \varphi_u(x_n)^{\alpha_n},$$

et donc φ_u stabilise les sous-espaces homogènes de $\mathbb{K}[x_1, \dots, x_n]$.

Démonstration. Si un morphisme φ_u existe, on a nécessairement : $\varphi_u(x_k) = \varphi_u \circ \iota(k) = u(k_x)$. Pour l'existence, il s'agit de constater que le morphisme φ caractérisé par l'application $f : \{1, \dots, n\} \to \mathbb{K}[x_1, \dots, x_n]$, $k \mapsto u(x_k)$ se restreint bien à u sur V^*, ce qui résulte de ce qu'un morphisme d'algèbres est en particulier linéaire. L'unicité vient de l'unicité dans le problème universel.

Reste à voir que c'est un automorphisme. Il n'y a qu'à constater que le morphisme $\varphi_{u^{-1}}$ est l'inverse de φ_u : en effet, leur composée est un morphisme d'algèbres qui se restreint en l'identité sur V^*, donc c'est l'identité (par unicité dans la première partie). □

[9] L'abus, c'est que les x_k étaient des indéterminées jusqu'à présent.

A.6. Remarque. On peut bien entendu remplacer V^* par un espace E, avec $u \in \mathrm{GL}(E)$ et définir ainsi une action de $\mathrm{GL}(E)$ sur l'algèbre de polynôme $\mathscr{S}(E)$. Le point de vue dual ne sert ici qu'à définir une action sur l'espace des fonctions polynomiales sur V.

Comme on peut le voir dans l'exemple qui suit, les calculs liés au prolongement sont très naturels.

A.7. Exemple. Supposons $V = \mathbb{K}^2$ et soit (x_1, x_2) la base canonique de la base duale de V. Soit $u(x_1) = ax_1 + bx_2$, $u(x_2) = cx_1 + dx_2$. Alors, l'action de φ_u sur l'espace des fonctions polynomiales de degré 2 sur V est donnée par

$$\begin{aligned}\varphi_u(x_1^2) &= a^2x_1^2 + 2abx_1x_2 + b^2x_2^2,\\ \varphi_u(x_1x_2) &= acx_1^2 + (ad+bc)x_1x_2 + bdx_2^2,\\ \varphi_u(x_2^2) &= c^2x_1^2 + 2cdx_1x_2 + d^2x_2^2.\end{aligned}$$

A.8. Remarque (Automorphismes de $\mathbb{K}[x_1, \ldots, x_n]$). Avec une seule indéterminée, il est facile de voir que tout automorphisme de $\mathbb{C}[x_1]$ est de la forme $x_1 \mapsto \alpha x_1 + \beta$ avec $(\alpha, \beta) \in \mathbb{K}^* \times \mathbb{K}$ (vérifiez !). Dès que l'on a au moins une variable de plus, on peut former les automorphismes *élémentaires*

$$(x_1, \ldots, x_k) \mapsto (x_1, \ldots, x_{i-1}, \alpha x_i + f, x_{i+1}, \ldots, x_n)$$

avec $\alpha \in \mathbb{K}^*$ et $f \in \mathbb{K}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$.

On dit qu'un automorphisme est *docile* (*tame*) s'il est produit d'automorphismes élémentaires. On sait depuis les années 40 et 50 que si $n = 2$, tout automorphisme de $\mathbb{K}[x_1, x_2]$ est docile ([42], [82] pour les *aficionados* et les sceptiques). En 1972, Nagata a conjecturé que l'automorphisme suivant de $\mathbb{K}[x_1, x_2, x_3]$ n'est pas docile :

$$(x_1, x_2, x_3) \mapsto \big(x_1 - 2(x_1x_3 + x_2^2)x_2 - (x_1x_3 + x_2^2)^2x_3,\ x_2 + (x_1x_3 + x_2^2)x_3,\ x_3\big).$$

Il a fallu attendre plus de trente ans avant que Shestakhov et Umirbaev ne le démontrent dans [77].

B. Exercices du chapitre VIII

B.1. Exercice (Théorème des deux carrés)

Soit p un nombre premier congru à 1 (mod 4). *On considère l'ensemble*

$$\Omega = \{(x,y,z) \in \mathbb{N}^3,\ x^2+4yz = p\}.$$

1. *Montrer que l'application*

$$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z), & \text{si } x < y-z, \\ (2y-x, y, x-y+z), & \text{si } y-z < x < 2y, \\ (x-2y, x-y+z, y), & \text{si } 2y < x, \end{cases}$$

est une involution (bien définie) de Ω, qui possède un unique point fixe.

Les triplets satisfaisant à $x < y-z$ et à $2y < x$ sont échangés. Pour le point fixe, on a donc : $y-z < x < 2y$. On le trouve avec l'hypothèse que p est premier, qui permet aussi d'écarter les situations $y-z = x$ et $x = 2y$.

2. *En déduire que l'involution $(x,y,z) \mapsto (x,z,y)$ possède au moins un point fixe et qu'il existe x et y entiers tels que $x^2+4y^2 = p$.*

Par la question précédente, le cardinal de Ω est impair et une involution sur un ensemble de cardinal impair a au moins un point fixe !

Nous remercions Cédric Bonnafé pour nous avoir signalé cet exercice, qui apparaît sous le numéro 1.3.6 dans [21]. Il s'agit d'une version améliorée par Don Zagier ([84], [50]) d'une preuve de Roger Heath-Broun [40] inspirée par Joseph Liouville. Le lien (ténu) avec le chapitre réside dans l'usage d'un groupe (deux actions de $\mathbb{Z}/2\mathbb{Z}$) pour résoudre une équation diophantienne.

B.2. Exercice (Invariants et quotient : des exemples)

1. *Pourquoi est-il raisonnable d'interpréter l'algèbre $\mathbb{C}[x_1,\dots,x_n]^{\mathfrak{S}_n}$ comme l'algèbre des « fonctions polynomiales » sur le quotient $\mathbb{C}^n/\mathfrak{S}_n$?*

2. *On fait agir $\mathbb{Z}$ sur $\mathbb{R}$ par translations et sur $\mathbb{R}[x]$ par : $(k\cdot F)(x) = F(x-k)$ pour $k \in \mathbb{Z}$ et $F \in \mathbb{R}[x]$. (On peut remplacer $\mathbb{R}$ par $\mathbb{C}$ si l'on préfère.) On voudrait que le quotient soit un « cercle », mais l'algèbre des invariants est : $\mathbb{R}[x]^{\mathbb{Z}} = \mathbb{R}$. Commenter.*

On pourra s'étendre sur la transcendance de l'exponentielle complexe ou critiquer le fait que $\mathbb{Z}$ n'est pas un sous-groupe algébrique de $\mathbb{R}$.

Les exemples suivants illustrent un principe général : « dans les bons cas », les polynômes invariants permettent de paramétrer les orbites fermées.

3. *On fait agir* $\mathbb{C}^*$ *sur* $\mathbb{C}^2$ *de la façon suivante :*

$$\forall \lambda \in \mathbb{C}^*,\ \forall (x,y) \in \mathbb{C}^2,\ \lambda \cdot (x,y) = (\lambda^{-1}x, \lambda y).$$

   (a) *Décrire les orbites de* $\mathbb{C}^*$*, préciser quelles sont les orbites fermées.*
   On trouvera une famille d'hyperboles, un point et deux axes épointés (non fermés).

   (b) *Décrire l'action correspondante de* $\mathbb{C}^*$ *sur les monômes de* $\mathbb{C}[X,Y]$*. Vérifier que l'on a :*

$$\mathbb{C}[X,Y]^{\mathbb{C}^*} = \mathbb{C}[XY] \simeq \mathbb{C}[T].$$

   On interprète $\mathbb{C}[T]$ comme l'algèbre des fonctions polynomiales sur la droite affine $\mathbb{C}$.

   (c) *Constater que chaque fibre de l'application* $\mathbb{C}^2 \to \mathbb{C}$, $(x,y) \mapsto xy$ *contient une unique orbite fermée.*
   Le principe est bien respecté.

4. *On fait agir* $\mathbb{C}^*$ *sur* $\mathbb{C}^2$ *de la façon suivante :*

$$\forall \lambda \in \mathbb{C}^*,\ \forall (x,y) \in \mathbb{C}^2,\ \lambda \cdot (x,y) = (\lambda x, \lambda y).$$

   Décrire les orbites de $\mathbb{C}^*$*, préciser celles qui sont fermées. Vérifier que l'on a :*

$$\mathbb{C}[X,Y]^{\mathbb{C}^*} = \mathbb{C}.$$

   Comme il n'y a qu'une seule orbite fermée, les invariants s'identifient bien aux fonctions sur un point. Le principe est respecté, mais c'est sans intérêt : pas assez d'orbites fermées, pas assez d'invariants.

5. *On fait agir* $\mathbb{C}^*$ *sur* $\mathbb{C} \times \mathbb{C}^*$ *de la façon suivante :*

$$\forall \lambda \in \mathbb{C}^*,\ \forall (x,y) \in \mathbb{C} \times \mathbb{C}^*,\ \lambda \cdot (x,y) = (\lambda x, \lambda y).$$

   (a) *Décrire les orbites de* $\mathbb{C}^*$*, vérifier qu'elles sont fermées.*

   (b) *Vérifier que l'on a :* $\mathbb{C}[X,Y,Y^{-1}]^{\mathbb{C}^*} = \mathbb{C}[XY^{-1}]$.

   (c) *Vérifier que les fibres de l'application* $\mathbb{C} \times \mathbb{C}^* \to \mathbb{C}$, $(x,y) \mapsto xy^{-1}$ *sont les orbites.*

   En restreignant l'action de 4, de nombreuses orbites sont devenues fermées. À présent, le principe est respecté, et ce n'est pas vide de sens.

6. *On fait agir* $\mathbb{C}$ *sur* $\mathbb{C}^2$ *par :* $t \cdot (x,y) = (x+ty, y)$ *pour* $t \in \mathbb{C}$, $(x,y) \in \mathbb{C}^2$.

   (a) *Décrire les orbites de* $\mathbb{C}$*; vérifier qu'elles sont toutes fermées.*

   (b) *Montrer que l'on a :* $\mathbb{C}[X,Y]^{\mathbb{C}} = \mathbb{C}[Y]$*. Constater que le « principe » n'est pas respecté.*

Il n'y a pas assez d'invariants pour décrire toutes les orbites fermées. Ici, on n'est pas dans un « bon cas » parce que le groupe n'agit pas de façon semi-simple sur $\mathbb{C}^2$ au sens de la définition X-A.13 : la droite stable n'a pas de supplémentaire stable.

7. *On fait agir le groupe orthogonal* $\mathrm{O}(n)$ *sur l'espace euclidien canonique* $\mathbb{R}^n$ *et ainsi,* $\mathrm{O}(n)$ *agit par automorphismes sur* $\mathbb{R}[x_1,\dots,x_n]$ *par*

$$g\cdot P(x)=P\big(g^{-1}(x)\big)\quad (g\in\mathrm{O}(n),\ P\in\mathbb{R}[x_1,\dots,x_n] \text{ et } x\in\mathbb{R}^n).$$

Soit $Q=x_1^2+\cdots+x_n^2\in\mathbb{R}[x_1,\dots,x_n]$. *Montrer que* $\mathbb{R}[x_1,\dots,x_n]^{\mathrm{O}(n)}=\mathbb{R}[Q]$. *Le « principe » est respecté.*

Pour l'inclusion non triviale, on montre d'abord en faisant agir des réflexions par rapport aux axes de coordonnées que tout polynôme P, $\mathrm{O}(n)$-invariant, est dans $\mathbb{R}[x_1^2,\dots,x_n^2]$. Pour y non nul dans $\mathbb{R}^n$, P est constant sur la sphère $\mathrm{O}(n)\cdot y$, et donc, la différentielle de $\mathrm{d}P_y$ s'annule sur l'espace tangent $y^\perp$ à la sphère. Il en suit que $\mathrm{d}P_y(h)=S(y)(y_1h_1+\cdots+y_nh_n)=S(y)\mathrm{d}Q_y(h)$ pour tout h. Or, la différentielle d'un polynôme invariant est encore invariante (utiliser par exemple l'unicité de la décomposition de Taylor). Donc, comme Q et P sont invariants, S est encore $\mathrm{O}(n)$-invariant. Tout est en place pour faire une récurrence (de deux en deux) sur le degré.

Mystery of the sages come into my realm of imagination.
Let me digest you.
Me'shell Ndegeocello, *Bittersweet*, 1996.

Chapitre IX

Sous-groupes finis de SO(3) et solides platoniciens

Dans ce chapitre assez classique, on établit la classique classification des sous-groupes finis de $\mathrm{SO}(3) = \mathrm{SO}_3(\mathbb{R})$. La méthode repose sur leur action sur la sphère-unité, plus précisément l'examen des orbites « spéciales » — celles qui ne sont pas de cardinal maximal. Dans les références classiques sur le sujet ([4] par exemple), on montre en général que l'une des ces orbites est un polyèdre régulier dont on a auparavant décrit le groupe de symétries, ce qui permet d'identifier le groupe.

Ici, bien que nous ayons déjà mené ce travail dans [H2G2, chapitre XII], nous faisons semblant de l'avoir oublié. Nous reconstruisons donc les sous-groupes, puis les polyèdres, sans présupposer la classification, ni l'étude, ni même l'existence de ces derniers. Nous retrouverons les solides platoniciens comme conséquence de la classification des sous-groupes. Bien sûr, construire un tétraèdre régulier ou un cube n'est pas un haut fait. C'est plus intéressant pour un icosaèdre : pour motiver l'approche, disons que l'examen des 2-Sylow d'un groupe particulier conduit naturellement aux coordonnées de ses douze sommets répartis en trois rectangles d'or.

Le prix à payer pour cette démarche, c'est que la preuve est moins compacte. Après une partie assez générale, dont la plupart des résultats sont classiques et ont même été déjà rencontrés dans cet ouvrage, nous allons établir une contrainte arithmétique sur les cardinaux des orbites des sous-groupes finis de SO(3) : c'est ce que capture le concept de *signature* d'un sous-groupe. Puis, après avoir classé les signatures possibles, nous établissons pour chacune qu'elle détermine le sous-groupe à conjugaison près.

La forme de la classification finale est bien connue : deux séries infinies dénombrables et trois cas exceptionnels. Cela n'est pas sans nous rappeler les carquois de type de représentation fini et les diagrammes de Dynkin du chapitre III ! Nous verrons au chapitre XI que ce n'est nullement un hasard.

1. Rappels

Dimension 1. On commence par rappeler quelques résultats classiques.

1.1. Proposition. *Tout sous-groupe de $\mathbb{R}$ est monogène ou dense.*

Démonstration. Soit G un sous-groupe de $\mathbb{R}$ non réduit à $\{0\}$. Soit $G^+ = G \cap \mathbb{R}^{+*}$ et soit $\alpha = \inf G^+$: le réel α est bien défini par le théorème de la borne supérieure. Deux cas se présentent.
Si $\alpha > 0$, alors G est $\mathbb{Z}\alpha$. Soit en effet x un élément de G et soit k la partie entière de x/α, alors : $k\alpha \leqslant x < (k+1)\alpha$, d'où : $0 \leqslant x - k\alpha < \alpha$. Or, $x - k\alpha$ est un élément de G. Par minimalité de α dans $G \cap \mathbb{R}^{+*}$, les inégalités précédentes donnent : $x - k\alpha = 0$. Autrement dit, G est contenu dans le groupe engendré par α. Dans ce cas, G est discret donc fermé, donc α appartient à G et il vient : $G = \mathbb{Z}\alpha$.
Sinon, on a : $\alpha = 0$. Montrons qu'alors G est dense dans $\mathbb{R}$. Soient x et y deux réels tels que $x < y$. Il s'agit de montrer que G contient un élément compris entre x et y. Notons $\varepsilon = y - x$. Comme la borne inférieure de $G \cap \mathbb{R}^{+*}$ est nulle, il existe un élément β de G tel que $0 \leqslant \beta < \varepsilon$. Soit k la partie entière de x/β, on a : $k\beta \leqslant x < (k+1)\beta$, d'où : $x \leqslant (k+1)\beta \leqslant k\beta + \beta \leqslant x + \varepsilon < y$. Ainsi, $(k+1)\beta$ appartient à G et à l'intervalle $]x, y[$, et G est dense. □

1.2. Corollaire. *Tout sous-groupe fini de $\mathbb{R}/2\pi\mathbb{Z}$ est monogène, engendré par (la classe modulo 2π de) $2\pi/n$, où n est son cardinal.*

Démonstration. Soit H un sous-groupe fini de $\mathbb{R}/2\pi\mathbb{Z}$ et $G = p^{-1}(H)$, où $p : \mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z}$ est la projection canonique. On vérifie sans peine que G est un sous-groupe de $\mathbb{R}$. La restriction de p à $[0,1]$ est injective : si G était dense, l'image de l'intersection $G \cap [0,1]$ serait une partie infinie de H, c'est absurbe[1]. D'après la proposition, G est donc monogène.

Soit α un générateur de G. D'après le théorème de Lagrange, on a : $n\alpha \equiv 0 \pmod{2\pi}$, où n est le cardinal de H. Ainsi, α vaut $2k\pi/n$ pour un entier k convenable. Avec l'identité de Bézout, on montre que le groupe engendré par α est aussi le groupe d'ordre n/d engendré par $2d\pi/n$, où d est le pgcd de k et n. Par suite, d vaut ± 1 et le corollaire est démontré. □

Sous-groupes finis en dimension 2. On fixe un plan euclidien P. On note $\mathrm{O}(P)$ le groupe des isométries de P, $\mathrm{SO}(P)$ le sous-groupe des isométries de déterminant 1, $\mathrm{O}_2(\mathbb{R})$ le groupe des matrices orthogonales 2×2, et $\mathrm{SO}_2(\mathbb{R})$ le groupe des matrices orthogonales 2×2 de déterminant 1, c'est-à-dire :

$$\mathrm{O}_2(\mathbb{R}) = \left\{A \in \mathscr{M}_2(\mathbb{R}),\ {}^tAA = \mathrm{Id}\right\}, \quad \mathrm{SO}_2(\mathbb{R}) = \left\{A \in \mathrm{O}_2(\mathbb{R}),\ \det A = 1\right\}.$$

[1] Pas d'inquiétude, c'était juste pour tester le correcteur d'orthographe.

Faits de base :

- le déterminant d'une isométrie est -1 ou 1 : en effet, si φ est une isométrie, on a : ${}^t\varphi\varphi = \mathrm{Id}_P$, donc $\det(\varphi)^2 = 1$;
- la donnée d'une base orthonormée $\mathbf{e}$ du plan euclidien P induit l'isomorphisme attendu $\mathrm{O}(P) \to \mathrm{O}_2(\mathbb{R})$, qui associe à une isométrie sa matrice dans $\mathbf{e}$; il se restreint à $\mathrm{SO}(P) \to \mathrm{SO}_2(\mathbb{R})$.

1.3. Lemme

(i) *Le groupe* $\mathrm{SO}_2(\mathbb{R})$ *est décrit par :*

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ; \quad a, b \in \mathbb{R},\ a^2 + b^2 = 1 \right\}.$$

(ii) *On a un isomorphisme*

$$\mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\sim} \mathrm{SO}_2(\mathbb{R}), \quad \theta \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

(iii) *Les isométries indirectes sont :*

$$\mathrm{O}_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ b & -a \end{pmatrix} ; \quad a, b \in \mathbb{R},\ a^2 + b^2 = 1 \right\}.$$

Démonstration. (i) Soit A un élément de $\mathrm{SO}_2(\mathbb{R})$. La première colonne de A est un vecteur de norme 1. Si on la note ${}^t(a\ b)$, on a donc : $a^2 + b^2 = 1$. Si ${}^t(c\ d)$ est la deuxième colonne de A, les réels c et d sont solutions du système

$$\begin{cases} ac + bd = 0, \\ -bc + ad = 1. \end{cases}$$

Le couple $(c, d) = (-b, a)$ est une solution et le déterminant de la matrice du système vaut 1, donc c'est la seule. Les éléments de $\mathrm{SO}_2(\mathbb{R})$ ont donc bien la forme annoncée. L'inclusion inverse est triviale.

(ii) C'est bien connu. On peut utiliser les tableaux de variations des fonctions cosinus et sinus ou bien les propriétés de l'exponentielle complexe.

(iii) Calculs analogues à ceux de l'assertion (i). □

1.4. Remarque. Les assertions (i) et (iii) sont valables sur tout corps.

1.5. Lemme

(i) *Tout sous-groupe fini de* $\mathrm{SO}_2(\mathbb{R})$ *est monogène, engendré par la rotation d'angle* $2\pi/n$, *où* n *est le cardinal du groupe.*

(ii) *Un sous-groupe fini de* $\mathrm{O}_2(\mathbb{R})$ *qui n'est pas contenu dans* $\mathrm{SO}_2(\mathbb{R})$ *est engendré par une rotation* ρ *d'angle* $2\pi/n$ ($n \in \mathbb{N}^*$) *et une réflexion* σ *satisfaisant à* $\sigma\rho\sigma^{-1} = \rho^{-1}$; *il est isomorphe au produit semi-direct* $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Pour prouver l'assertion (i), on se ramène à $\mathbb{R}/2\pi\mathbb{Z}$ par le lemme 1.3 (ii) et l'on applique le corollaire 1.2.

Prouvons (ii). Soit H un sous-groupe de $O_2(\mathbb{R})$ qui n'est pas contenu dans $SO_2(\mathbb{R})$. Alors, $H^+ = H \cap SO_2(\mathbb{R})$ est un sous-groupe d'indice 2 de H. En effet, le déterminant induit un isomorphisme de H/H^+ sur $\{-1,1\}$. On fixe une rotation ρ engendrant H^+, on note n son ordre (l'ordre de H^+ ou de ρ, c'est pareil). On fixe une réflexion $\sigma \in H \setminus H^+$. On vérifie directement que $\sigma\rho\sigma^{-1} = \rho^{-1}$. On vérifie par ailleurs que H^+ et $H^+\sigma = \{\rho^k\sigma,\ k = 0,\dots,n-1\}$ forment une partition de H, et le reste « coule de source ».

Dimension 3 : une rotation à la fois. On note SO(3) le groupe des matrices orthogonales 3×3, qui s'identifie au groupe des isométries directes de $\mathbb{R}^3$ euclidien standard, dans lequel on note $\langle\cdot,\cdot\rangle$ le produit scalaire.

1.6. Lemme. *Soit ρ une isométrie directe de $\mathbb{R}^3$ euclidien standard.*

(i) *L'ensemble des valeurs propres réelles de ρ contient* 1 *et il est contenu dans* $\{-1,1\}$.

(ii) *L'espace des points fixes,* $\ker(\rho - \mathrm{Id})$, *est de dimension* 1 *ou* 3.

(iii) *Il existe un réel θ et une base orthonormée de $\mathbb{R}^3$ dans laquelle la matrice de ρ est :*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

On appelle les éléments de SO(3) des *rotations.* L'*axe* d'une rotation différente de l'identité est la droite formée par ses points fixes.

Démonstration. (i) Soit λ une valeur propre réelle de ρ et soit v un vecteur propre associé. Comme ρ est une isométrie, la relation $\rho(v) = \lambda v$ entraîne : $||v|| = ||\rho(v)|| = |\lambda|\,||v||$, d'où $|\lambda| = 1$, puis $\lambda = \pm 1$.

Notons λ_1, λ_2, λ_3 les valeurs propres complexes de ρ répétées avec multiplicité. Montrons que l'une d'entre elles vaut 1. Si toutes trois sont réelles, la relation $\lambda_1\lambda_2\lambda_3 = \det\rho = 1$ entraîne que l'une des trois vaut 1 : en effet, $(-1)^3 = -1$. Si l'une des valeurs propres est complexe non réelle, disons λ_1, alors sa conjuguée $\overline{\lambda_1}$ est aussi valeur propre ; mais alors, la troisième valeur propre est l'inverse du produit des deux premières, c'est-à-dire $1/|\lambda_1|^2$, qui est un réel strictement positif.

(ii) Comme le déterminant de ρ vaut 1, si l'on a $\dim\ker(\rho - \mathrm{Id}) \geqslant 2$, alors 1 est valeur propre triple de ρ et l'on en déduit que ρ est une transvection. Comme c'est aussi une isométrie, c'est l'identité. En effet, si (e_1, e_2, e_3) est une base orthonormée de $\mathbb{R}^3$ dans laquelle e_1 et e_2 sont propres pour ρ, on peut écrire $\rho(e_3) = e_3 + ae_1 + be_2$ pour a, b réels convenables. La condition $||\rho(e_3)|| = ||e_3||$ et l'orthonormalité de la base donnent alors : $a = b = 0$.

(iii) Désormais, on suppose que que $\ker(\rho - \mathrm{Id})$ est une droite – l'axe de ρ. Fixons un vecteur e_1 de norme 1 dans cette droite. Notons P le plan orthogonal à l'axe de ρ et montrons que P est stable par ρ. Il suffit de montrer que pour $v \in P$, $\rho(v)$ est orthogonal à e_1 :

$$\langle \rho(v), e_1 \rangle = \langle \rho(v), \rho(e_1) \rangle = \langle v, e_1 \rangle = 0.$$

De plus, la restriction de ρ à P est dans $\mathrm{SO}(P)$. En effet, le déterminant de ρ est le produit des déterminants des restrictions de ρ à $\ker(\rho - \mathrm{Id})$ et à P. Choisissons une base orthonormée (e_2, e_3) de P. Pour l'orientation du plan P définie par cette base, la restriction de ρ est une rotation de P, dont on note θ l'angle. La matrice de ρ est donc $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$ dans la base (e_1, e_2, e_3). □

1.7. Remarque. Le réel θ n'est défini qu'au signe près (et à 2π près). En revanche, $\cos\theta$ ne dépend que de ρ puisque l'on a : $\mathrm{tr}\,\rho = 1 + 2\cos\theta$.

1.8. Exemple. Les éléments d'ordre 2 de $\mathrm{SO}(3)$ sont les rotations d'angle π. Une rotation est d'ordre 2 si et seulement si sa trace vaut -1. On appelle *demi-tours* ces rotations.

1.9. Formule des classes et cardinal du quotient

Soit G un groupe fini opérant sur un ensemble fini $\mathscr{P}$. On note G_p le stabilisateur d'un point $p \in \mathscr{P}$ et $\mathscr{P}^g$ l'ensemble des points fixes d'un éléments $g \in G$. Notons que le cardinal $|G_p|$ ne dépend que de l'orbite de p, car, par le principe de conjugaison, tous les stabilisateurs sont conjugués ($G_{g\cdot p} = gG_pg^{-1}$ pour tout g de G).

1.10. Proposition (Formule de Burnside). *Soit G un groupe fini opérant sur un ensemble fini $\mathscr{P}$. Alors :*

$$|\mathscr{P}| = \sum_{\mathbf{p} \in \mathscr{P}/G} \frac{|G|}{|G_p|} \quad \text{et} \quad |\mathscr{P}/G| = \frac{1}{|G|} \sum_{g \in G} |\mathscr{P}^g|.$$

Dans la première somme, $\mathbf{p}$ parcourt l'ensemble des orbites de G dans $\mathscr{P}$ et p désigne un point quelconque de $\mathbf{p}$.

Démonstration. La première formule se déduit de la partition de $\mathscr{P}$ en orbites et, pour chaque orbite $G \cdot p$, des bijections orbitales $G/G_p \to G \cdot p$, $gG_p \mapsto g \cdot p$:

$$|\mathscr{P}| = \sum_{p \in \mathscr{P}} 1 = \sum_{\mathbf{p} \in \mathscr{P}/G} \sum_{p \in \mathbf{p}} 1 = \sum_{\mathbf{p} \in \mathscr{P}/G} |\mathbf{p}| = \sum_{\mathbf{p} \in \mathscr{P}/G} \frac{|G|}{|G_p|}.$$

Pour montrer la seconde formule, on évalue de deux façons la somme double

$$S = \sum_{g\in G}\sum_{p\in\mathscr{P}} \delta_{gp,p},$$

où $\delta_{gp,p}$ vaut 1 si g fixe p et 0 sinon.

Pour g fixé, les p tels que $\delta_{gp,p} = 1$ sont les points fixes de g ; pour p fixé, les g tels que $\delta_{gp,p} = 1$ sont les éléments du stabilisateur G_p de p. On a donc :

$$\sum_{g\in G} |\mathscr{P}^g| = S = \sum_{p\in\mathscr{P}} |G_p| = \sum_{p\in\mathscr{P}} \frac{|G|}{|G\cdot p|} = \sum_{\mathbf{p}\in\mathscr{P}/G}\sum_{p\in\mathbf{p}} \frac{|G|}{|\mathbf{p}|} =$$

$$= \sum_{\mathbf{p}\in\mathscr{P}/G} |G| = |G|\,|\mathscr{P}/G|.$$

□

1.11. Remarque. La seconde formule est la célèbre *formule de Burnside.* On l'a déjà vue à l'œuvre (sous une forme pondérée) dans la théorie des coloriages, voir le lemme V-5.18 et on en verra une preuve alternative à base de représentations dans la proposition X-B.15.

2. Sous-groupes finis de SO(3) : signature

2.1. Notations, remarques utiles

On fixe un sous-groupe fini G de SO(3), non réduit à $\{\mathrm{Id}\}$. On appelle *pôle* d'une rotation $g \in \mathrm{SO}(3)$ d'angle non nul ($g \neq \mathrm{Id}$), un des deux points d'intersection de l'axe de la rotation g et de la sphère-unité $\mathscr{S}$, de centre l'origine et de rayon 1 (chaque rotation non triviale possède donc deux pôles). On note $\mathscr{P}$ l'ensemble des pôles des éléments de $G \setminus \{\mathrm{Id}\}$.

Comme G est fini et qu'une rotation différente de l'identité possède deux pôles, l'ensemble $\mathscr{P}$ est fini. De plus, si p est un pôle de $g \in G \setminus \{\mathrm{Id}\}$ et si $h \in G$, alors $h(p)$ est fixé par $hgh^{-1} \in G \setminus \{\mathrm{Id}\}$, d'où : $h(p) \in \mathscr{P}$. Ainsi, $\mathscr{P}$ est stable par G.

Pour tout pôle $p \in \mathscr{P}$, on a : $-p \in \mathscr{P}$. Les stabilisateurs de p et $-p$ coïncident. Par conséquent, si le stabilisateur d'un pôle p est le seul stabilisateur ayant un cardinal cardinal donné (c'est-à-dire que $|G_p| \neq |G_q|$ si p et q ne sont pas dans la même orbite), on peut en déduire que p et $-p$ sont dans la même orbite.

Le stabilisateur d'un pôle p est un sous-groupe cyclique puisqu'il stabilise le plan orthogonal à ce pôle : la restriction à ce plan définit une injection de G_p dans le groupe spécial orthogonal du plan.

L'isobarycentre d'une orbite de G dans $\mathscr{P}$ est fixe par G. Si l'orbite contient au moins deux pôles non opposés, cela entraîne que ce barycentre est l'origine (c'est la seule intersection des axes d'éléments des stabilisateurs).

On note $r = |\mathscr{P}/G|$; $\omega_1, \ldots, \omega_r$ les orbites de G dans $\mathscr{P}$; $n_1, \ldots, n_r$ les cardinaux des stabilisateurs de ces orbites ($n_i = |G_p|$ pour $p \in \omega_i$). On pose enfin : $N = |G|$.

2.2. Définition. On appelle *signature* d'un sous-groupe fini de SO(3) la liste $(N ; n_1, \ldots, n_r)$.

2.3. Remarque. Quitte à gâcher la surprise, indiquons à l'avance le sens des nombres n_i lorsqu'il y a trois orbites de pôles ($r = 3$). Pour un solide platonicien, sujet déjà rencontré dans [H2G2, chapitre XII], l'axe d'une rotation qui le laisse fixe passe par un sommet, le milieu d'une arête ou le centre d'une face. Les trois orbites que nous allons trouver dans le cadre de ces solides correspondent à cette classification (arête-sommet-centre, les deux derniers étant susceptibles d'être échangés par dualité), les n_i sont les ordres des stabilisateurs des trois types de points ou, si l'on préfère, les N/n_i sont les nombres d'arêtes, de sommets et de centres de faces. Ces points spéciaux doivent être vus dans $\mathscr{P}$, c'est-à-dire qu'ils sont normalisés pour appartenir à la sphère.

Ceci étant admis, l'examen de la caractéristique d'Euler-Poincaré, qui force l'égalité $S-A+F = 2$ (voir, par exemple, [H2G2, théorème XII-2.3]), donne une équation portant sur la somme alternée $N/n_1 - N/n_2 + N/n_3$ et pas la somme des N/n_i qui va apparaître incessamment.

2.4. Remarque. Pour tout i entre 1 et r, le groupe G contient (au moins) un élément d'ordre n_i, à savoir le générateur du stabilisateur (d'un pôle appartenant à l'orbite correspondante), voir le lemme 1.5.

2.5. Proposition (Équation caractéristique). *Soit G un sous-groupe fini de* SO(3) *de cardinal N, soit r le nombre d'orbites de pôles de G et soient $n_1, \ldots, n_r$ les cardinaux des stabilisateurs des orbites de pôles. Alors, on a :*

$$\sum_{i=1}^{r} \left(1 - \frac{1}{n_i}\right) = 2 - \frac{2}{N}.$$

Démonstration. Par définition des pôles, si $p \in \mathscr{P}$, il existe un élément $g \in G$ différent de l'identité dont l'axe contient p, si bien que l'on a : $G_p \neq \{\mathrm{Id}\}$, ou encore : $n_i \geqslant 2$ pour tout i entre 1 et r.

Pour $g \in G$ différent de l'identité, on a : $|\mathscr{P}^g| = 2$; si $g = \mathrm{Id}$, on a : $|\mathscr{P}^g| = |\mathscr{P}|$. L'équation aux classes s'écrit :

$$|\mathscr{P}| = \sum_{i=1}^{r} \frac{N}{n_i}\cdot$$

D'autre part, le calcul de $|\mathscr{P}/G|$, par la formule de Burnside, donne :

$$Nr = |G|\,|\mathscr{P}/G| = |\mathscr{P}| + \sum_{g\neq \mathrm{Id}} |\mathscr{P}^g| = |\mathscr{P}| + 2(N-1).$$

On en déduit :

$$\sum_{i=1}^{r} \frac{N}{n_i} = |\mathscr{P}| = Nr - 2(N-1),$$

égalité que l'on récrit sous la forme voulue :

$$\sum_{i=1}^{r} \left(1 - \frac{1}{n_i}\right) = 2 - \frac{2}{N}\cdot$$ □

2.6. Remarque. On renvoie le lecteur à une jolie preuve alternative de ce résultat dans [55], très en lien avec la notion d'homographie. En voici l'idée clé : comme $\mathrm{SO}_3(\mathbb{R})$ est inclus dans $\mathrm{SO}_3(\mathbb{C})$, qui est isomorphe à $\mathrm{PSL}_2(\mathbb{C})$, on peut voir G comme un sous-groupe[2] de $\mathrm{PSL}_2(\mathbb{C})$, et donc, agissant par homographies sur le corps $\mathbb{C}(X)$ des fractions rationnelles. Par le théorème de Lüroth (voir la remarque VII-1.7), le corps $\mathbb{C}(X)^G$ est isomorphe à $\mathbb{C}(j)$ pour une fraction rationnelle j bien choisie, unique à homographie près. L'égalité que nous venons de montrer découle alors du calcul, par deux méthodes différentes, du nombre de zéros de la dérivée j' de la fraction j.

On va à présent résoudre l'équation caractéristique.

2.7. Proposition. *Soit G un sous-groupe fini non trivial de* $\mathrm{SO}(3)$ *de cardinal N, soit r le nombre d'orbites de pôles de G et soient $n_1, \ldots, n_r$ les cardinaux des stabilisateurs des orbites de pôles. Alors, la signature de G est l'une des suivantes :*

- *soit $r = 2$ et $(N\,; n_1, n_2) = (N\,; N, N)$;*
- *soit $r = 3$ et $(N\,; n_1, n_2, n_3) = (2n\,; 2, 2, n)$, pour un entier $n \geqslant 2$ convenable ;*
- *soit $r = 3$ et $(N\,; n_1, n_2, n_3) = (12\,; 2, 3, 3)$;*
- *soit $r = 3$ et $(N\,; n_1, n_2, n_3) = (24\,; 2, 3, 4)$;*
- *soit $r = 3$ et $(N\,; n_1, n_2, n_3) = (60\,; 2, 3, 5)$.*

[2] Et, plus précisément, $\mathrm{SO}_3(\mathbb{R})$ s'envoie, via l'isomorphisme exceptionnel, sur $\mathrm{PSU}_2(\mathbb{C})$, voir [H2G2, exercice IX-2.2].

On a : $r \leqslant 3$. En effet, l'inégalité $n_i \geqslant 2$ valable pour tout i, amène à une contradiction :

$$\frac{r}{2} = \sum_{i=1}^{r} \left(1 - \frac{1}{2}\right) \leqslant \sum_{i=1}^{r} \left(1 - \frac{1}{n_i}\right) = 2 - \frac{2}{N} < 2.$$

On a : $r \geqslant 2$. En effet, si l'on avait $r = 1$, l'équation caractéristique serait :

$$1 - \frac{1}{n_1} = 2 - \frac{2}{N}, \quad \text{d'où } \frac{N}{n_1}(n_1 + 1) = 2.$$

Puisque n_1 est le cardinal d'un sous-groupe de G, N/n_1 est un entier, on en déduirait : $n_1 + 1 \leqslant 2$, ce qui est incompatible avec : $n_1 \geqslant 2$.

Si $r = 2$, alors $n_1 = n_2 = N$. En effet, ordonnons n_1 et n_2 de sorte que $n_1 \leqslant n_2 \leqslant N$. Si l'on suppose $n_1 < N$, on a :

$$\frac{1}{n_1} + \frac{1}{n_2} > \frac{2}{N}, \quad \text{d'où } 1 - \frac{1}{n_1} + 1 - \frac{1}{n_2} < 2 - \frac{2}{N},$$

ce qui contredit l'équation caractéristique.

Désormais, on suppose $r = 3$. Il s'agit de résoudre

$$1 + \frac{2}{N} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3},$$

avec, par exemple, $n_1 \leqslant n_2 \leqslant n_3$.

On a : $n_1 = 2$. En effet, si $n_1 \geqslant 3$, alors

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} \leqslant \frac{3}{n_1} \leqslant 1,$$

ce qui est impossible. Puisque $n_1 \geqslant 2$, on peut conclure que $n_1 = 2$.

On a : $2 \leqslant n_2 \leqslant 3$. En effet, si l'on suppose que $n_2 \geqslant 4$, on aboutit à une contradiction par :

$$\frac{1}{n_2} + \frac{1}{n_3} \leqslant \frac{2}{n_2} \leqslant \frac{1}{2}.$$

Si $n_2 = 2$, l'équation caractéristique devient : $2/N = 1/n_3$. On obtient ainsi une famille infinie de solutions : $N = 2n$, $n_1 = 2$, $n_2 = 2$, $n_3 = n$, avec $n \in \mathbb{N}^*$ quelconque.

Si $n_2 = 3$, l'équation caractéristique devient : $(N + 12)n_3 = 6N$. Comme n_3 est le cardinal d'un sous-groupe de G, c'est un diviseur de N. Notons $d_3 = N/n_3$, on en déduit que d_3 divise 12. On exclut les cas $d_3 \in \{1, 2\}$ (ce qui donne $N \leqslant 0$) et $d_3 = 3$ (ce qui donne $n_3 = 2 < 3 = n_2$). Il reste trois cas très intéressants :

$$\begin{array}{llll} N = 12\,; & n_1 = 2, & n_2 = 3 & n_3 = 3, \\ N = 24\,; & n_1 = 2, & n_2 = 3 & n_3 = 4, \\ N = 60\,; & n_1 = 2, & n_2 = 3 & n_3 = 5. \end{array}$$

3. Existence et unicité des sous-groupes de signature donnée

Dans ce paragraphe, on prouve que pour chaque signature mise en évidence dans la proposition 2.7, il existe un sous-groupe de SO(3), unique à conjugaison près, qui a cette signature. On le décrit comme groupe abstrait et, lorsque c'est adapté, on construit un polyèdre régulier dont il est le groupe de symétries. Voici un énoncé chapeau qui sera précisé dans (et démontré par) les propositions 3.2, 3.4, 3.8, 3.10 et 3.11. Pour G sous-groupe fini de SO(3), on conserve les notations de la partie précédente.

3.1. Proposition. *Soit σ l'une des signatures de la proposition 2.7, c'est-à-dire l'un des triplets $(N\,;n_1,n_2)$ ou des quadruplets $(N\,;n_1,n_2,n_3)$. Il existe une et une seule classe de conjugaison de sous-groupes de* SO(3) *ayant pour signature σ.*

On procède signature par signature, en commençant par les deux séries infinies.

3.2. Proposition. *Pour N entier naturel non nul, il existe une et une seule classe de conjugaison de sous-groupes de signature $(N\,;N,N)$: ce sont les groupes cycliques engendrés par un élément d'ordre N.*

Démonstration. Soit G un sous-groupe de signature $(N\,;N,N)$. Il y a $r=2$ orbites dans $\mathscr{P}$ et le cardinal des orbites est : $N/n_1 = N/n_2 = 1$, c'est-à-dire que chaque orbite est un singleton. Il y a donc exactement deux pôles, nécessairement antipodaux. Cela signifie que tous les éléments de G ont le même axe. En particulier, ils stabilisent le plan orthogonal à cet axe et la restriction à ce plan est injective.

On a vu que le groupe des isométries directes d'un plan possède exactement un sous-groupe fini de tout ordre, qui est cyclique : par suite, G est cyclique, et voici la matrice d'un générateur dans une base convenable :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\dfrac{2\pi}{N} & -\sin\dfrac{2\pi}{N} \\ 0 & \sin\dfrac{2\pi}{N} & \cos\dfrac{2\pi}{N} \end{pmatrix}.$$

Réciproquement, pour tout entier non nul N, il existe des sous-groupes finis de SO(3) ayant pour signature $(N\,;N,N)$ et ils sont tous conjugués par un élément de SO(3). □

Avant de passer à la signature $(N\,;2,2,n)$, voici un lemme géométrique utile.

3.3. Lemme. *Deux demi-tours σ_1 et σ_2, en dimension 3, commutent si et seulement si leurs axes sont orthogonaux ou confondus.*

Démonstration. Supposons que σ_1 et σ_2 commutent. Alors, σ_2 stabilise les espaces propres de σ_1. Mais, les seules droites stables par σ_2 sont son axe et les droites du plan qui lui sont orthogonales : l'axe de σ_1 est donc l'axe de σ_2 ou bien il lui est orthogonal. Voici une autre démarche : comme il s'agit d'involutions, la commutation s'écrit : $\sigma_1 = \sigma_2\sigma_1\sigma_2^{-1}$. Par le principe de conjugaison, l'axe de σ_1 est égal à son image par σ_2 ; on conclut comme ci-dessus. La réciproque est immédiate. □

3.4. Proposition. *Pour n entier, $n \geqslant 2$, il existe une et une seule classe de conjugaison de sous-groupes de signature $(2n\,;2,2,n)$: ce sont des groupes diédraux, engendrés par une rotation d'angle $2\pi/n$ et un demi-tour d'axes orthogonaux.*

Démonstration. Soit G un groupe de signature $(2n\,;2,2,n)$. L'ensemble $\mathscr{P}$ des pôles contient $2n+2$ éléments répartis dans les trois orbites.

Supposons que $n = 2$. Alors, l'ordre de G est 4, et G est donc abélien. Dans chaque orbite de pôles, le stabilisateur est d'ordre 2. Notons σ_i $(1 \leqslant i \leqslant 3)$ les éléments d'ordre 2 dans le stabilisateur de l'orbite ω_i. Comme on a trois orbites, il y a au moins deux éléments d'ordre 2 d'axes différents, disons σ_1 et σ_2 pour fixer les notations.

D'après le lemme 3.3, les éléments σ_1 et σ_2 ont des axes orthogonaux. Dans une base orthonormée convenable, leurs matrices sont, respectivement :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On constate que $\sigma_3 = \sigma_1\sigma_2$ est le demi-tour ayant pour axe la perpendiculaire commune aux deux axes. De plus, deux groupes ayant cette signature sont conjugués.

Désormais, on suppose que $n \geqslant 3$. Fixons $p \in \omega_3$. Comme il n'y a qu'un seul stabilisateur de cardinal n, les pôles p et $-p$ sont dans la même orbite et comme le cardinal de ω_3 est $N/n = 2$, on a : $\omega_3 = \{p, -p\}$.

Le fixateur H de p est, comme tout stabilisateur d'un pôle, un sous-groupe cyclique de G ; il est d'ordre n et d'indice 2. On oriente le plan orthogonal à p et l'on appelle ρ le générateur de H d'angle $2\pi/n$.

Par ailleurs, on fixe un élément $q \in \omega_1$. L'élément non trivial du stabilisateur de q est un demi-tour σ d'axe $\mathbb{R}q$. Puisque p et $-p$ sont dans la même orbite ω_3, le point q n'appartient pas à l'axe $\mathbb{R}p$ de ρ ; par suite, σ ne fixe pas p. En revanche, $\sigma(p)$ appartient à ω_3 donc $\sigma(p) = -p$, d'où q appartient au plan orthogonal à $\mathbb{R}p$.

Complétons (p,q) en une base orthonormée (p,q,r). Quitte à remplacer r par $-r$ pour des raisons d'orientation, les matrices de σ et ρ sont donc :

$$\Sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ 0 & \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

On se convainc sans peine que les $\rho^k(q)$ $(k = 0, \dots, n-1)$ constituent ω_1, que $\sigma\rho\sigma^{-1} = \rho^{-1}$, etc. Bref, G est un groupe diédral.

Deux groupes ayant cette signature sont conjugués : d'après la description précédente, ils ont les mêmes générateurs à changement de base près.

Enfin, il existe de tels groupes : c'est un calcul de routine que de montrer que les deux matrices Σ et P ci-dessus engendrent un groupe de signature $(2n\,;2,2,n)$. □

Constatons d'après la proposition 2.7 que les sous-groupes d'ordre 4 (resp. 8) de SO(3) ont pour signature $(4\,;2,2)$ ou $(4\,;2,2,2)$ (resp. $(8\,;2,2,4)$). On peut en déduire la proposition suivante, qui sera utile pour étudier les 2-Sylow de sous-groupes plus gros.

3.5. Proposition (Sous-groupes d'ordre 4 et 8). *Il y a deux classes de conjugaison de sous-groupes d'ordre* 4 *dans* SO(3) *:*

- *les sous-groupes cycliques engendrés par une rotation d'angle* $\pi/2$ *;*
- *les sous-groupes isomorphes à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *engendrés par deux demi-tours d'axes orthogonaux.*

Il y a une classe de conjugaison de sous-groupes d'ordre 8 *dans* SO(3) *: un tel sous-groupe est engendré par une rotation d'angle* $\pi/2$ *et un demi-tour d'axes orthogonaux.*

3.6. Groupe du tétraèdre, symétries « du » n-simplexe régulier

On va montrer que les groupes (éventuels) de signature $(12\,;2,3,3)$ sont les groupes des isométries directes des tétraèdres réguliers. On commence par un résultat d'existence et d'unicité de cet objet géométrique en toute dimension.

Soit n un entier non nul, et soit $\mathscr{E}$ un espace affine euclidien de dimension n. Une partie S de cardinal $n+1$ est appelée *n-simplexe régulier* de côté d (où $d \in \mathbb{R}^{+*}$) si deux points quelconques de S sont à distance d l'un de l'autre :

$$\forall (p,q) \in S^2, \quad ||\overrightarrow{pq}|| = d.$$

Par exemple, un 1-simplexe régulier est un segment, un 2-simplexe régulier est un triangle équilatéral, un 3-simplexe régulier un tétraèdre régulier.

3.7. Lemme. *Dans un espace affine euclidien de dimension $n \geqslant 1$, il existe exactement une orbite de n-simplexes réguliers de côté 1 sous l'action du groupe des isométries.*

De plus, le groupe des isométries qui préserve un n-simplexe régulier est isomorphe au groupe des permutations de $n+1$ lettres. La restriction de l'action à l'ensemble des sommets du n-simplexe établit un tel isomorphisme.

Démonstration. On laisse le cas $n = 1$ en exercice. Pour $n = 2$, c'est un « cas d'égalité des triangles », qui se ramène à un calcul simple. D'une part, il existe au moins un triangle équilatéral, par exemple celui dont les sommets ont, dans un repère orthonormé, pour coordonnées $q_0 = (0,0)$, $q_1 = (1,0)$ et $q_2 = (1/2, \sqrt{3}/2)$.

D'autre part, si le triangle $p_0p_1p_2$ est équilatéral de côté 1, on a (Al-Kashi !) :

$$\langle \overrightarrow{p_0p_1}, \overrightarrow{p_0p_2} \rangle = \frac{||\overrightarrow{p_0p_1}||^2 + ||\overrightarrow{p_0p_2}||^2 - ||\overrightarrow{p_1p_2}||^2}{2} = \frac{1}{2}.$$

Par suite, la matrice du produit scalaire euclidien dans les bases $(\overrightarrow{q_0q_1}, \overrightarrow{q_0q_2})$ et $(\overrightarrow{p_0p_1}, \overrightarrow{p_0p_2})$ coïncident, ce qui signifie que l'application affine qui envoie q_i sur p_i (pour $0 \leqslant i \leqslant 2$) est une isométrie : ainsi, deux triangles équilatéraux sont dans la même orbite.

Soit n quelconque. Considérons $\mathbb{R}^{n+1}$ euclidien standard, pour lequel la base canonique $(e_0, \ldots, e_n)$ est orthonormée, et le sous-espace affine euclidien H défini par l'équation

$$x_0 + \cdots + x_n = \frac{1}{\sqrt{2}}.$$

Dans H, les vecteurs $\{q_0, \ldots, q_n\}$, où $q_i = e_i/\sqrt{2}$ pour tout i, forment un n-simplexe régulier de côté 1.

Soit $\{p_0, \ldots, p_n\}$ un n-simplexe régulier. Comme les triangles $p_0p_ip_j$ $(0 < i < j)$ sont tous équilatéraux, la matrice du produit scalaire dans la base $(\overrightarrow{p_0p_i})_{1 \leqslant i \leqslant n}$ est formée de 1 sur la diagonale et de 1/2 ailleurs : c'est la même que dans la base $(\overrightarrow{q_0q_i})_{1 \leqslant i \leqslant n}$. Par suite, l'application affine qui envoie le repère affine $(q_j)_{0 \leqslant j \leqslant n}$ sur $(p_j)_{0 \leqslant j \leqslant n}$ est une isométrie. Il y a donc exactement une orbite de n-simplexes sous l'action des isométries.

Comme un n-simplexe régulier est un repère affine, la restriction d'une isométrie à l'ensemble des sommets est injective. Inversement, le même argument que ci-dessus prouve que l'application affine associée à une permutation π des sommets préserve la matrice du produit scalaire : c'est donc une isométrie. (En effet, les triangles $q_{\pi(0)}q_{\pi(i)}q_{\pi(j)}$ sont équilatéraux.)

Cela prouve la proposition dans H. Mais, comme tous les espaces affines euclidiens de dimension n sont isométriques, le résultat s'étend à tous les espaces affines. □

3.8. Proposition (Groupe du tétraèdre). *Il existe une seule classe de conjugaison de sous-groupes de* SO(3) *ayant pour signature* $(12;2,3,3)$. *Un tel groupe est isomorphe au groupe alterné* $\mathfrak{A}_4$, *et c'est le groupe des isométries directes qui préservent un tétraèdre régulier.*

Démonstration. Soit G un groupe de signature $(12;2,3,3)$. Soit $p \in \omega_2$. Le stabilisateur G_p de p est d'ordre $n_2 = 3$: il est donc engendré par une rotation ρ d'ordre 3. L'axe de ρ intersecte $\mathscr{S}$ et, *a fortiori*, ω_2 en deux points au plus. Comme l'orbite de p sous G a pour cardinal $12/3 = 4$, l'un au moins des trois points de $\{q,r,s\} = \omega_2 \setminus \{p\}$ n'est pas fixé par ρ : son stabilisateur dans G_p est trivial donc G_p permute librement les trois points de $\{q,r,s\}$.

En examinant l'effet d'une rotation d'ordre 3 sur un point situé hors de son axe, on voit que les points q, r, s forment un triangle équilatéral inclus dans un plan affine orthogonal à p. Comme p était arbitraire dans ω_2, trois points quelconques de ω_2 forment un triangle équilatéral. Ainsi, la distance entre deux points de ω_2 est égale à un réel d fixé. D'après le lemme, cela signifie que ω_2 est un tétraèdre régulier.

L'action de G sur ω_2 donne un morphisme $G \to \mathfrak{S}_4$. Comme les quatre points de ω_2 ne sont pas tous dans un même plan, ce morphisme est injectif. Or, $\mathfrak{S}_4$ possède un unique sous-groupe d'indice 2, c'est $\mathfrak{A}_4$. D'où : $G \simeq \mathfrak{A}_4$.

Le lemme entraîne qu'il n'y a qu'un seul tétraèdre régulier à similitude près : une similitude qui envoie un tétraèdre régulier sur un autre conjugue leurs groupes de symétries et, par suite, l'unique sous-groupe d'indice 2 d'icelui. Cela prouve la proposition. □

3.9. Remarque. Pour référence ultérieure, notons que l'on a : $-p \notin \omega_2$, donc $-p \in \omega_3$, puis $\omega_3 = -\omega_2$ (utiliser la commutation de G avec $-\mathrm{Id}$). De plus, $\omega_2 \cup \omega_3$ est l'ensemble des pôles des éléments d'ordre 3 de G.

3.10. Proposition (Groupe du cube). *Il existe une seule classe de conjugaison de sous-groupes de* SO(3) *ayant pour signature* $(24;2,3,4)$. *Un tel groupe est isomorphe au groupe symétrique* $\mathfrak{S}_4$ *et c'est le groupe des isométries directes qui préservent un cube.*

Démonstration. On s'intéresse aux groupes (éventuels) de signature $r = 3$, $N = 24$, $n_1 = 2$, $n_2 = 3$, $n_3 = 4$.

L'orbite ω_2 a pour cardinal $24/3 = 8$. Comme elle est seule de ce cardinal, elle est symétrique : $-\omega_2 = \omega_2$. On peut donc regrouper ces huit points en quatre paires de points antipodaux, ce qui fournit un morphisme $G \to \mathfrak{S}_4$ défini par : $g \cdot \{p,-p\} = \{g(p),-g(p)\}$ pour $g \in G$ et $p \in \omega_2$. On peut aussi considérer les droites engendrées par ces paires, et dire que G agit (transitivement) sur quatre droites.

On veut montrer que ce morphisme est injectif. Choisissons $p \in \omega_2$ et $g \in G_p$ non trivial. L'existence d'un tel élément d'ordre $n_2 = 3$ entraîne que les quatre droites ne sont pas coplanaires (le seul plan stable par g est orthogonal à l'axe), et même que trois d'entre elles engendrent $\mathbb{R}^3$. Or, si une application linéaire admet quatre directions propres dans cette configuration, c'est une homothétie. Cela prouve l'injectivité.

Au bilan : $G \simeq \mathfrak{S}_4$.

Notons que ω_2 est l'ensemble des pôles des éléments de G d'ordre 3. Si H désigne le sous-groupe de G isomorphe à $\mathscr{A}_4$, remarquons que H contient tous les éléments d'ordre 3 de G, donc les éléments de ω_2 sont des pôles de H, et plus précisément, ce sont les pôles des éléments d'ordre 3 de H. D'après le paragraphe précédent, l'action de H sur ω_2 contient deux orbites de cardinal 4, formant deux tétraèdres réguliers symétriques par rapport à l'origine —ils forment un cube.

À présent, si G et G' sont deux sous-groupes de SO(3) de signatures respectives $(24\,;2,3,4)$, l'isométrie directe qui envoie un des deux tétraèdres de G sur un des deux tétraèdres de G' conjugue le sous-groupe d'indice 2 de G en celui de G'. □

3.11. Proposition (Groupe de l'icosaèdre). *Soit G un sous-groupe de* SO(3) *de signature* $(60\,;2,3,5)$. *Alors, G est isomorphe au groupe alterné $\mathfrak{A}_5$ et il est conjugué au groupe de symétries de l'icosaèdre régulier dont les douze sommets ont pour coordonnées dans une base orthonormée (avec $\phi = (1+\sqrt{5})/2$) :*

$$(0, \pm 1, \pm\phi), \quad (\pm\phi, 0, \pm 1), \quad (\pm 1, \pm\phi, 0).$$

Résumé de la preuve. On montre que G possède cinq 2-sous-groupes de Sylow. L'action par conjugaison sur les 2-Sylow induit un isomorphisme $G \to \mathfrak{A}_5$. Dans un système de coordonnées dont les axes sont les axes des éléments d'un 2-Sylow, les points de ω_3 sont ceux annoncés dans la proposition.

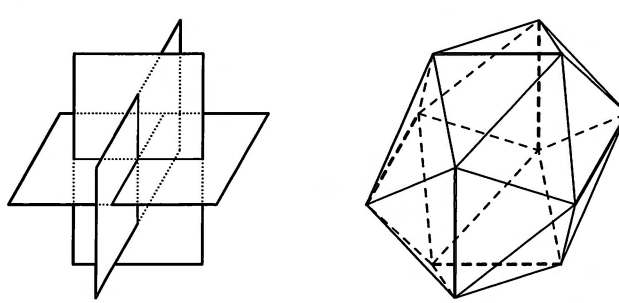


Figure 3.1. *Trois rectangles d'or dans un icosaèdre*

Démonstration. Soit G un sous-groupe de signature $r = 3$, $N = 60$, $n_1 = 2$, $n_2 = 3$, $n_3 = 5$.

Les 2-sous-groupes de Sylow de G sont isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En effet, ils sont de cardinal 4 et G ne contient pas d'élément d'ordre 4 (sinon, un stabilisateur aurait un ordre n_i multiple de 4), on peut invoquer la proposition 3.5.

Inversement, fixons un élément d'ordre 2, donc son axe D, et cherchons les éléments d'ordre 2 qui commutent avec lui : il ne peut en exister plus de deux. En effet, s'il y en avait au moins un troisième, il y aurait deux demi-tours d'axes orthogonaux à D mais non orthogonaux entre eux, dont le produit serait une rotation d'axe D, mais pas d'ordre 2. Impossible, car le stabilisateur des éléments de $D \cap \mathscr{S}$ sont d'ordre 2. Plus simplement, le stabilisateur d'un pôle associé à un élément d'ordre 2 est d'ordre $4 = 60/(30/2)$, donc le centralisateur de cet élément est d'ordre 4. Ainsi, tout élément d'ordre 2 appartient à un unique 2-Sylow.

L'orbite ω_1, seule orbite de ce cardinal, contient $N/n_1 = 60/2 = 30$ éléments : il se regroupent en quinze paires de points opposés, ce qui définit quinze droites, chacune étant l'axe d'un demi-tour. Comme les stabilisateurs des autres pôles sont de cardinal impair, G contient quinze éléments d'ordre 2. Comme un élément d'ordre 2 appartient à un unique 2-Sylow et qu'un 2-Sylow contient trois éléments d'ordre 2, le nombre de 2-Sylow est $15/3 = 5$, soit cinq triplets de droites deux à deux orthogonales. Entre parenthèses, le normalisateur d'un 2-Sylow a donc pour cardinal $N/N_2 = 60/5 = 12$, c'est un sous-groupe tétraédral ; ces cinq sous-groupes sont les groupes d'isométries des cinq tétraèdres que l'on peut construire dans un dodécaèdre régulier ; mais ne nous emballons pas.

En faisant agir G sur ses 2-Sylow, on obtient un morphisme $G \to \mathfrak{S}_5$. Montrons que cette action est libre (*i.e.* le morphisme injectif). En effet, le noyau K de l'action étant l'intersection des normalisateurs des 2-Sylow, il a pour ordre un diviseur de 12. Vu qu'un élément d'ordre 2 n'appartient qu'à un seul 2-Sylow, K n'en contient aucun. Si K contenait un élément g d'ordre 3, il contiendrait g^{-1} et, K étant distingué, les conjugués de g. Or, l'orbite ω_2, associée aux éléments d'ordre $n_2 = 3$, contient $60/3 = 20$ points ; ils se regroupent deux par deux en dix axes de rotations d'ordre 3, soit vingt éléments d'ordre 3 en tout ; un élément h de G qui envoie un de ces axes sur l'axe de g conjugue une telle rotation en g ou g^{-1}. Si K contenait g, il contiendrait vingt éléments d'ordre 3 : c'est beaucoup trop pour que le quotient G/K, dont l'ordre serait alors au plus 3, puisse agir transitivement sur les 2-Sylow.

Ainsi, G s'identifie à l'unique sous-groupe d'ordre 60 de $\mathfrak{S}_5$, *i.e.* : $G \simeq \mathfrak{A}_5$.

À présent, nous allons déterminer les coordonnées des points de ω_3 dans une base dont les axes sont les axes d'un 2-Sylow. Cela prouvera l'unicité de G à conjugaison près dans $\mathrm{SO}(3)$ et permettra de prouver l'existence de sous-groupes ayant la signature voulue.

Comme ω_3 est la seule orbite de cardinal 12, elle est stable par antipodie : choisissons un point p de ω_3, il existe g_1 dans G tel que $g_1 \cdot p = -p$. Alors, comme -1 est une valeur propre de g_1, on peut affirmer que g_1 est une involution. Soient g_2 et $g_3 = g_1 g_2$ les deux autres involutions du 2-Sylow S contenant g_1. Rappelons que g_1, g_2 et g_3 sont trois demi-tours d'axes orthogonaux.

L'action de S sur ω_3 est libre, car le stabilisateur des points de ω_3, de cardinal impair, ne contient aucun des g_i. Par suite, ω_3 est la réunion de trois orbites de cardinal 4. Plus précisément, puisque g_2 commute à g_1, les points $\pm g_2 \cdot p$ appartient au plan $\ker(g_1 + \mathrm{Id})$. Ainsi, une des orbites de S dans ω_3 est le rectangle[3] de sommets p, $-p$, $g_2 \cdot p$ et $-g_2 \cdot p$, contenu dans le plan $\ker(g_1 + \mathrm{Id})$. Aucun de ces sommets n'appartient à $\ker(g_2 + \mathrm{Id})$ car l'intersection de ces deux plans est l'axe de g_3 ; idem pour $\ker(g_3 + \mathrm{Id})$. Comme g_2 et g_3 sont conjugués à g_1, on obtient que ω_3 est la réunion de trois rectangles contenus dans les plans $\ker(g_i + \mathrm{Id})$.

Les axes des g_i forment un trièdre rectangle dont les plans de coordonnées sont justement les plans $\ker(g_i + \mathrm{Id})$. Choisissons plus précisément une base qui engendre ces axes. Soit e_1 un vecteur normé de l'axe de g_1 ($e_1 \in \omega_1$). Le normalisateur du 2-Sylow S est d'ordre 12, il contient un élément d'ordre 3 que l'on note h. Cet élément ne stabilise pas la droite engendrée par e_1 donc il l'envoie sur $\mathbb{R}e_2$ ou $\mathbb{R}e_3$. Quitte à remplacer h par h^2, on peut supposer que $h \cdot e_1$ est fixé par g_2. On pose $e_2 = h \cdot e_1$ et $e_3 = h^2 \cdot e_1$. Alors $\mathbf{e} = (e_1, e_2, e_3)$ est une base orthonormée de $\mathbb{R}^3$. La matrice de h dans $\mathbf{e}$ est une matrice de permutation.

Le rectangle $S \cdot p$ contient un point p_1 de coordonnées $(0, a, b)$, où a et b sont des réels strictement positifs. L'action de S et de h, c'est-à-dire du normalisateur de S, donne les coordonnées des douze points de ω_3 :

$$(0, \pm a, \pm b), \quad (\pm a, \pm b, 0), \quad (\pm b, 0, \pm a).$$

Soit $p_2 = g_2 \cdot p_1$ le point de coordonnées $(0, a, -b)$. Le stabilisateur de p_1 contient un élément k d'ordre 5. L'image p_3 de p_2 par k n'est pas dans le plan $\ker(g_1 + \mathrm{Id})$, d'où :

$$(2b)^2 = ||\overrightarrow{p_1 p_2}||^2 = ||\overrightarrow{p_1 p_3}||^2 = a^2 + b^2 + (a + \varepsilon b)^2,$$

[3]Deux points sur le cercle-unité et leurs symétriques par rapport au centre du cercle forment un rectangle.

où ε vaut ± 1. Le rapport (positif) $x = a/b$ est donc solution de :

$$x^2 + \varepsilon x - 1 = 0, \quad i.e.\ x = \frac{-\varepsilon + \sqrt{5}}{2}.$$

Soit $\phi = (1+\sqrt{5})/2$ le nombre d'or, x vaut donc ϕ ou ϕ^{-1}. À produit par un scalaire près, les points de ω_3 ont donc pour coordonnées :

$$\begin{cases} (0, \pm\phi, \pm 1), & (\pm\phi, \pm 1, 0), & (\pm 1, 0, \pm\phi) \\ \text{ou} \quad (0, \pm\phi^{-1}, \pm 1), & (\pm\phi^{-1}, \pm 1, 0), & (\pm 1, 0, \pm\phi^{-1}). \end{cases}$$

La première famille s'obtient de la seconde en multipliant par ϕ et en permutant e_2 et e_3 : les deux parties ont donc des groupes d'isométrie isomorphes. (Plus haut, changer le signe de ε revenait à permuter a et b.)

On vient de prouver qu'à changement de base orthonormée et homothétie près, ω_3 s'identifie à la partie I à douze éléments décrite dans la proposition. Il en résulte que G est conjugué à un sous-groupe de symétrie de I. En fait, il y a nécessairement égalité puisque la signature de G en fait un sous-groupe maximal parmi les sous-groupes de SO(3). Pour prouver que tous les sous-groupes de signature $(60; 2, 3, 5)$ sont conjugués et qu'il en existe, il suffit donc de prouver que le groupe de symétrie de I contient un élément d'ordre 5. Pour cela, il suffit de calculer la matrice des rotations d'angle $\pm 2\pi/5$ d'axe porté par un point quelconque de I et de vérifier qu'elle préserve I. Ce calcul de routine est laissé en exercice. □

En conclusion, nous avons prouvé le théorème suivant.

3.12. Théorème. *Soit G un sous-groupe fini de* SO(3). *Alors, G est isomorphe à l'un des suivants : groupe cyclique $\mathfrak{C}_n = \mathbb{Z}/n\mathbb{Z}$ $(n \geqslant 1)$, groupe diédral $\mathfrak{D}_n$ $(n \geqslant 2)$, $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$.*

De plus, deux sous-groupes de SO(3) *qui sont isomorphes sont conjugués par un élément de* SO(3).

A. Exercices du chapitre IX

Voici deux exercices égarés du tome premier.

A.1. Exercice. *Un icosaèdre et un dodécaèdre sont inscrits dans une même sphère. Montrer qu'ils sont alors circonscrits à une même sphère.*

Penser à la dualité !

Cet exercice, qui nous a été signalé par Bodo Lass, a été posé au Tournoi des villes *en 2005* (`http://tournoidesvilles.fr`).

A.2. Exercice. *On place les douze sommets d'un icosaèdre régulier sur la surface de la Terre, avec un sommet au pôle Nord.*

1. Estimer *laquelle des latitudes suivantes est la plus proche de celle des cinq sommets de l'hémisphère nord autres que le pôle :*
   - *le cercle polaire arctique à* 66.56° ;
   - *le tripoint Belgique-France-Luxembourg à* 49.5° ;
   - *le Jbel Toubkal, à* 31.1° ;
   - *le tropique du Cancer, à* 23.44° *?*
2. Calculer *la latitude exacte de ces sommets, en supposant que la Terre est une sphère parfaite.*

Cet exercice, dû à Elwyn Berlekamp et Joe P. Buhler, est tiré du numéro de juin 2014 du magazine Emissary, *édité par le Mathematical Science Research Institute.*

A.3. Exercice (Classification des sous-groupes finis de $\mathrm{O}_3(\mathbb{R})$)

On veut classer les sous-groupes finis de $\mathrm{O}_3(\mathbb{R})$, *à partir de ceux de* $\mathrm{SO}_3(\mathbb{R})$. *Soit donc* $\tilde{\Gamma}$ *un sous-groupe fini de* $\mathrm{O}_3(\mathbb{R})$ *qui n'est pas contenu dans* $\mathrm{SO}_3(\mathbb{R})$.

1. *Vérifier que la restriction du déterminant est une surjection de* $\tilde{\Gamma}$ *sur* $\{1,-1\}$ *et que son noyau est* $\Gamma = \tilde{\Gamma} \cap \mathrm{SO}_3(\mathbb{R})$.
2. *Montrer que si* $-\mathrm{I}_3 \in \tilde{\Gamma}$, *alors* $\tilde{\Gamma} \simeq \Gamma \times \mathbb{Z}/2\mathbb{Z}$.

   Par $-1 \mapsto -\mathrm{I}_3$, on définit une section du déterminant, puis l'on applique [H2G2, corollaire II-5.3.4] ; le produit est en fait direct, car $-\mathrm{I}_3$ commute avec tout $\tilde{\Gamma}$.
3. *On suppose ici que* $-\mathrm{I}_3 \notin \tilde{\Gamma}$. *Soit* $g \in \tilde{\Gamma} \setminus \Gamma$. *Montrer que* $\tilde{\Gamma} = \Gamma \cup g\Gamma$, *et que* $\hat{\Gamma} = \Gamma \cup (-g\Gamma)$ *est un sous-groupe de* $\mathrm{SO}_3(\mathbb{R})$ *qui contient* Γ *comme sous-groupe d'indice* 2.

   On vérifie que $\hat{\Gamma}$ est stable par le produit en faisant quatre cas.
4. *Montrer que les sous-groupes finis de* $\mathrm{SO}_3(\mathbb{R})$ *contenant un sous-groupe d'indice* 2 *sont isomorphes à* $\mathbb{Z}/2n\mathbb{Z}$, $\mathfrak{D}_n$ *(pour un entier* n*) ou* $\mathfrak{S}_4$.

Le groupe $\mathfrak{A}_5$ est simple et, dans le groupe $\mathfrak{A}_4$, un sous-groupe d'ordre 3 ne stabilise aucun sous-groupe propre du groupe de Klein.

5. *Réciproquement, soit* $\hat{\Gamma}$ *un sous-groupe fini de* $\mathrm{SO}_3(\mathbb{R})$ *contenant un sous-groupe* Γ *d'indice* 2, *et soit* k *tel que* $\hat{\Gamma} = \Gamma \cup k\Gamma$. *Vérifier que* $\tilde{\Gamma} = \Gamma \cup (-k\Gamma)$ *est un sous-groupe fini de* $\mathrm{O}_3(\mathbb{R})$ *qui n'est pas dans* $\mathrm{SO}_3(\mathbb{R})$.

6. *Soit* $\tilde{\Gamma}$ *un sous-groupe de* $\mathrm{O}_3(\mathbb{R})$. *Montrer pour conclure que l'on est dans l'une ou l'autre des situations suivantes :*
   - $\tilde{\Gamma} \simeq \Gamma \times \mathbb{Z}/2\mathbb{Z}$, *où* $\Gamma = \tilde{\Gamma} \cap \mathrm{SO}_3(\mathbb{R})$;
   - *le couple* $\left(\tilde{\Gamma}, \tilde{\Gamma} \cap \mathrm{SO}_3(\mathbb{R})\right)$ *est de la forme* $(\mathbb{Z}/2n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$, $(\mathfrak{D}_n, \mathbb{Z}/n\mathbb{Z})$, $(\mathfrak{D}_{2n}, \mathfrak{D}_n)$ *(avec* n *entier positif) ou* $(\mathfrak{S}_4, \mathfrak{A}_4)$.

And in the odd chance there are any
Astronomy aficionados amongst you,
the North Star is... that one.
Quentin Tarantino, *Django unchained*, 2012.

Chapitre X

Sous-groupes finis de $\mathbf{SO_3(\mathbb{R})}$ et théorie des représentations

Dans ce court chapitre, suivi d'une longue annexe présentant la théorie des représentations, on voit comment utiliser cette théorie pour construire à nouveau de façon explicite les sous-groupes de $\mathrm{SO}(3) = \mathrm{SO}_3(\mathbb{R})$ ainsi que les polyèdres réguliers.

En effet, la donnée d'un groupe fini G et d'une représentation dans un espace vectoriel réel, assimilé à un espace affine pointé en 0, fournit des orbites finies $G \cdot P$, où P est un point de l'espace. Par une méthode classique, le groupe G agit par isométries pour une forme euclidienne sur l'espace. On peut alors associer à une telle orbite un polyèdre, inscrit dans une sphère, défini comme l'enveloppe convexe des points de cette orbite. En général, ce polyèdre n'est pas régulier, même s'il possède de belles propriétés. Mais, pour certains choix (de groupe, de représentation et de point P), on peut trouver, grâce à de miraculeuses coïncidences numériques, des polyèdres réguliers. On se propose de construire ainsi, via des représentations de dimension 3 bien choisies, les solides platoniciens, déjà maintes fois discutés.

« Pourquoi se donner tant de mal ? », se demandera l'étudiant en manque de motivation. En effet, il n'y a pas grand mystère à construire un cube (ses sommets sont les points de coordonnées $(\pm 1, \pm 1, \pm 1)$ dans une base orthonormée) ou un tétraèdre régulier (prendre un sommet sur deux par arête sur le cube précédent). Il sera toutefois agréable d'associer des objets simples et bien digérés comme le cube et le tétraèdre à la plus abstraite, plus récente et beaucoup plus générale théorie des représentations — ici, des groupes $\mathfrak{S}_4$ et $\mathfrak{A}_4$.

Et pour la construction de l'icosaèdre (et du dodécaèdre), on va prouver l'existence d'un sous-groupe de $SO_3(\mathbb{R})$ isomorphe à $\mathfrak{A}_5$, sans l'étude fine de l'action sur la sphère-unité du chapitre précédent (signature, action des 2-Sylow...). Le calcul des coordonnées des sommets de l'icosaèdre est plus difficile ; de fait, si le calcul des caractères permet de manipuler avec aisance et élégance les représentations d'un groupe, il ne permet pas directement d'en calculer explicitement les matrices. On verra deux méthodes qui illustrent d'autres principes généraux de la théorie.

Ce chapitre s'appuie donc sur un bagage élémentaire, certes, mais assez consistant de théorie des représentations, que nous préférons rappeler en annexe A. D'une part, nous y exposerons la problématique de la théorie : comment construire explicitement des représentations (à partir d'actions de groupes, par somme directe, espaces de morphismes...), comment les classer, et comment les ramener à un objet de calcul simple, le caractère. D'autre part, l'étude des solides platoniciens nous amènera à étudier des aspects plus subtils de la théorie des représentations : la réalisation d'un caractère en une représentation sur $\mathbb{R}$.

1. Tétraèdre régulier et cube

La construction-express des représentations de dimension 3 de $\mathfrak{A}_4$ et $\mathfrak{S}_4$ exploite l'action naturelle de ces groupes sur $\{1,2,3,4\}$, qui induit une représentation irréductible de degré 3. Nous utilisons ici à son maximum la construction de représentations associée à une action de groupe, et un critère qui établit son irréductibilité, voir A et en particulier B.14 et E.

1.1. « Construction » « du » tétraèdre régulier

Considérons le groupe alterné $\mathfrak{A}_4$. Il agit sur $X = \{1,2,3,4\}$ et l'action est deux fois transitive. Notons à ce propos un fait classique.

Exercice. *Pour n entier supérieur à 2, le groupe $\mathfrak{A}_n$ agit de façon $n-2$ transitive sur $\{1,\dots,n\}$.*

Une $(n-2)$-liste $(a_1,\dots,a_{n-2})$ d'éléments deux à deux distincts peut être envoyée sur une autre par un élément de $\mathfrak{S}_n$. Si cet élément est dans $\mathfrak{A}_n$, c'est gagné ; sinon, on le compose à droite par la transposition (a_{n-1},a_n), où a_{n-1} et a_n sont les deux éléments restants de $\{1,\dots,n\}$.

La représentation réelle V_X mise en évidence en E.2 est donc irréductible. Par acquit de conscience (ou simplement par pur plaisir !), on calcule facilement son caractère χ.

nom classe	1	2_1	3
représentant	Id	(12)(34)	(123)
ordre éléments	1	2	3
cardinal	1	3	8
χ	3	-1	0

Et l'on vérifie que $\langle \chi, \chi \rangle = 1$. Choisissons sur V_X un produit scalaire (euclidien, on est sur $\mathbb{R}$), que l'on peut, quitte à moyenner, choisir invariant par $\mathfrak{A}_4$ (voir E). Prenons une base orthonormée de V_X ; l'action de $\mathfrak{A}_4$ sur X fournit donc un morphisme $\rho : \mathfrak{A}_4 \to \mathrm{O}_3(\mathbb{R})$. De plus, on voit sur la table qu'il est injectif : si $\rho(g) = \mathrm{Id}$, alors $\chi(g) = 3$, et donc $g = \mathrm{Id}$.

Soit g un 3-cycle de $\mathfrak{A}_4$. Alors, les valeurs propres de $\rho(g)$ sont trois racines cubiques de l'unité, et l'on vérifie que son déterminant, qui est produit des trois valeurs propres, ne peut être alors égal à -1. Ainsi, $\rho(g) \in \mathrm{SO}_3(\mathbb{R})$.

Exercice. *Pour une preuve alternative du fait que $\rho(g) \in \mathrm{SO}_3(\mathbb{R})$, on peut se rappeler que la représentation de $\mathfrak{A}_4$ sur V_X est la restriction d'une représentation de $\mathfrak{S}_4$ et utiliser le fait que $\mathfrak{A}_4$ est le groupe dérivé de $\mathfrak{S}_4$. Préciser.*

Maintenant, comme $\mathfrak{A}_4$ est engendré par les 3-cycles, le morphisme ρ envoie $\mathfrak{A}_4$ dans $\mathrm{SO}_3(\mathbb{R})$.

Les huit 3-cycles de $\mathfrak{A}_4$ se regroupent en quatre paires de la forme $\{g, g^2\}$, ce qui fournit, via ρ, quatre axes pour les rotations correspondantes. Puisque deux 3-cycles provenant de paires distinctes ne commutent pas, les quatre axes sont bien distincts. On obtient donc exactement huit points d'intersection de ces quatre axes avec la sphère-unité de l'espace euclidien V_X.

Soient h et g dans $\mathfrak{A}_4$ et soit Δ_g l'axe de la rotation $\rho(g)$. Alors, $\rho(h)(\Delta_g)$ est l'axe $\Delta_{hgh^{-1}}$ de la rotation $\rho(hgh^{-1})$: c'est en effet une droite invariante. Ainsi, $\mathfrak{A}_4$ agit sur l'ensemble de ces huit points. Soit P l'intersection de Δ_g avec la sphère. Montrons que l'orbite $\mathfrak{A}_4 \cdot P$ fournit quatre sommets d'un solide platonicien, c'est-à-dire d'un tétraèdre. Le stabilisateur de P dans $\mathfrak{A}_4$ contient un 3-cycle g, et donc il contient $\{\mathrm{Id}, g, g^2\}$. Si h est un élément de $\mathfrak{A}_4$ n'appartenant pas à $\{\mathrm{Id}, g, g^2\}$, il ne commute pas à g, et donc $\rho(h)(P) \neq P$ (cela impliquerait que $\rho(h)$ est une rotation d'axe Δ, et comme ρ est injective, h commuterait avec g). On a donc bien quatre éléments dans l'orbite de P et de plus, comme le stabilisateur de P n'est autre que $\mathfrak{A}_3$, l'action de $\mathfrak{A}_4$ sur les quatre sommets s'identifie à l'action naturelle de $\mathfrak{A}_4$ sur quatre objets, qui est doublement transitive. Et donc, comme $\mathfrak{A}_4$ agit de façon doublement transitive par isométries, deux points distincts quelconques sont à la même distance. On a bien construit un tétraèdre régulier.

1.2. « Construction » de l'octaèdre (et du cube, par dualité)

Nous l'avons déjà dit : il n'y a pas grand prodige à construire un cube. Il reste toutefois intéressant de développer des méthodes de constructions de polyèdres par la théorie des représentations, qui ne demande que ça.

Considérons le groupe symétrique $\mathfrak{S}_4$; il agit sur $X = \{1, 2, 3, 4\}$ et l'action est deux fois transitive. La représentation réelle V_X du paragraphe E.2 est donc irréductible, et l'on calcule facilement son caractère χ :

nom classe	1	2_1	3	2_2	4
représentant	Id	(12)(34)	(123)	(12)	(1234)
ordre éléments	1	2	3	2	4
cardinal	1	3	8	6	6
χ	3	-1	0	1	-1

Une nouvelle fois, on vérifie que l'on a : $\langle \chi, \chi \rangle = 1$. Choisissons sur V_X un produit scalaire invariant par $\mathfrak{S}_4$, prenons une base orthonormée de V_X, nous obtenons un morphisme $\rho : \mathfrak{S}_4 \to O_3(\mathbb{R})$. Les transpositions ont pour image des involutions de trace 1, donc leur spectre est $(-1, 1, 1)$: pas de chance, l'image n'est pas dans $SO_3(\mathbb{R})$. On ne peut donc pas appliquer la même méthode que pour $\mathfrak{A}_4$.

Qu'à cela ne tienne : multiplions chaque matrice par la signature. On vérifie en une ligne que l'on définit une nouvelle représentation[1]

$$\check{\rho} : \mathfrak{S}_4 \to O_3(\mathbb{R}), \quad g \mapsto \varepsilon(g)\rho(g),$$

dont le caractère est :

nom classe	1	2_1	3	2_2	4
représentant	Id	(12)(34)	(123)	(12)	(1234)
$\check{\chi}$	3	-1	0	-1	1

On constate que les transpositions sont envoyées sur des matrices de spectre $(-1, -1, 1)$, c'est-à-dire sur des demi-tours : la représentation est à valeurs dans $SL_3(\mathbb{R})$. Bien sûr, les restrictions de ρ et $\check{\rho}$ à $\mathfrak{A}_4$ coïncident avec la représentation par permutation ci-dessus.

À partir de là, la méthode ressemble à celle utilisée pour le tétraèdre. Les six 4-cycles de $\mathfrak{S}_4$ se répartissent en trois paires de la forme $\{g, g^3\}$, et des arguments de commutation montrent que les axes des rotations sont distincts. On a donc exactement six points d'intersection de ces axes avec

[1] C'est un cas particulier de produit tensoriel, voir le paragraphe XI-A.3.

la sphère-unité, dont on veut montrer qu'ils forment les sommets d'un polyèdre régulier. Comme pour le groupe alterné, le groupe $\mathfrak{S}_4$ agit sur l'ensemble de ces six points et le stabilisateur d'un point est égal au sous-groupe engendré par un 4-cycle. Si l'on prend une paire de points non opposés, on voit facilement que son stabilisateur dans $\mathrm{SO}_3(\mathbb{R})$ est constitué de l'identité et du retournement autour de l'axe passant par le milieu de ces deux points. Donc, le stabilisateur d'une telle paire dans $\mathfrak{S}_4$, qui agit par rotation, est d'ordre inférieur à 2. Comptons ces paires, il y en a $\binom{6}{2} - 3 = 12$ et donc, $\mathfrak{S}_4$ agit transitivement sur ces paires. Les autres paires sont des paires de points opposés et donc ne peuvent constituer une arête du polyèdre. Ainsi, nous avons construit six points de la sphère qui forment un polyèdre dont les arêtes sont toutes de même longueur. Il s'agit bien d'un solide platonicien, qui n'est rien d'autre que l'octaèdre régulier.

On se contentera d'affirmer, en laissant la preuve en exercice : les huit intersections des axes des 3-cycles avec la sphère-unité sont les sommets d'un cube. De plus, les douze intersections des axes des transpositions et de la sphère-unité sont les sommets d'un cuboctaèdre.

2. L'icosaèdre et son groupe de symétrie

Dans cette partie, pas d'action naturelle sur quatre objets comme pour les constructions précédentes. Dommage, car elle avait pour avantage, outre une certaine naturalité, de fournir une représentation réelle. On utilise donc les représentations de $\mathfrak{A}_5$ pour le plonger dans $\mathrm{SO}_3(\mathbb{R})$, via une opération délicate :

1. la construction de la table des caractères prouve l'existence de deux morphismes $\mathfrak{A}_5 \to \mathrm{GL}_3(\mathbb{C})$;
2. il s'agit donc de voir si ce morphisme se factorise en $\mathfrak{A}_5 \to \mathrm{GL}_3(\mathbb{R}) \to \mathrm{GL}_3(\mathbb{C})$, ce qui est une question non triviale (E.3) ; on en donne trois preuves : par un critère abstrait dû à Schur et deux constructions tensorielles ; de là, il est facile de prouver l'existence d'un produit scalaire invariant et d'en déduire un morphisme $\mathfrak{A}_5 \to \mathrm{O}_3(\mathbb{R})$, puis $\mathfrak{A}_5 \to \mathrm{SO}_3(\mathbb{R})$;
3. enfin, on s'intéresse à la construction effective des matrices de la représentation, ce qui fait l'objet d'un TP sur ordinateur (pour manipuler soixante matrices 3×3, *hey*, à quoi vous attendiez-vous ?).

2.1. Table des caractères complexes de $\mathfrak{A}_5$

Avant d'attaquer la table des caractères de $\mathfrak{A}_5$, on décrit ses classes de conjugaison.

Exercice

1. *Montrer que les deux 5-cycles* (12345) *et* (12354) *ne sont pas dans la même classe de conjugaison pour* $\mathfrak{A}_5$.
   Soit $\tau = (45)$. S'il existait σ dans $\mathfrak{A}_5$ tel que $\sigma(12345)\sigma^{-1} = \tau(12345)\tau^{-1}$, alors $\tau\sigma$ centraliserait un 5-cycle, donc en serait un, donc serait pair...
2. *Montrer que* $\mathfrak{A}_5$ *possède cinq classes de conjugaison.*
   Partir des classes de conjugaison de $\mathfrak{S}_5$ incluses dans $\mathfrak{A}_5$, puis chercher le stabilisateur (donc le centralisateur) d'un élément par classe.

On a cinq classes de conjugaison, baptisées par l'ordre des éléments :

nom classe	1	2	3	5_1	5_2
représentant	Id	(12)(34)	(123)	(12345)	(12354)
ordre éléments	1	2	3	5	5
cardinal	1	15	20	12	12

On veut donc construire cinq caractères irréductibles. Pas grand-chose à dire sur le caractère trivial, noté 1. L'action naturelle de $\mathfrak{A}_5$ sur cinq lettres est doublement transitive (et même triplement, comme on l'a vu en 1.1), ce qui donne un caractère irréductible de degré 4, noté ϕ (proposition B.15).

nom classe	1	2	3	5_1	5_2
1	1	1	1	1	1
ϕ	4	0	1	-1	-1

On sait, par exemple par [H2G2, proposition VIII-3.1], que $\mathfrak{A}_5$ est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_5)$, d'où une action transitive sur les six points de la droite projective. De plus, on sait grâce à [H2G2, chapitre VII] que l'action de $\mathrm{PSL}_2(\mathbb{K})$ sur $\mathbb{P}^1$ est doublement transitive, et même triplement. Il existe donc un morphisme injectif $\varphi : \mathfrak{A}_5 \to \mathfrak{S}_6$ et la représentation V_X associée à cette action, de degré 5, est irréductible par la proposition B.15. Soit θ le caractère (irréductible, donc) de cette représentation ; on se propose de calculer θ.

Comme $\mathfrak{A}_5$ est simple et que le morphisme φ n'est pas trivial, il est injectif. De plus, comme $\mathfrak{A}_5$ est simple non abélien, il est égal à son groupe dérivé et φ est à valeurs dans le groupe dérivé de $\mathfrak{S}_6$, c'est-à-dire $\mathfrak{A}_6$.

L'image d'un 5-cycle par φ est un élément d'ordre 5, c'est donc un 5-cycle dans $\mathfrak{A}_6$: il y a donc un point fixe unique dans l'action sur six lettres et les éléments de 5_1 et 5_2 annulent θ, par la proposition B.15. De même, un produit de deux transpositions est d'ordre 2 et donc, il a pour image un élément d'ordre 2 de $\mathfrak{A}_6$, c'est-à-dire un produit de deux transpositions.

Cette image possède donc deux points fixes. Encore une fois, par B.15, la valeur de θ en un produit de deux transpositions est 1.

L'image d'un 3-cycle est donc un élément d'ordre 3 : c'est un produit de deux 3-cycles ou un 3-cycle. Donc, soit il n'a pas de point fixe et θ prend la valeur -1, soit il possède trois points fixes et θ prend la valeur 2. Par irréductibilité, le caractère θ est de norme 1, et un calcul donne la valeur cherchée : -1. On a calculé θ :

nom classe	1	2	3	5_1	5_2
θ	5	1	-1	0	0

On a trouvé trois caractères irréductibles distincts (1, ϕ et θ). Par le corollaire C.8, il en reste encore deux à exhiber. Notons $d_1 \leqslant d_2$ les degrés des caractères manquants. On a : $d_1^2 + d_2^2 + 1^2 + 4^2 + 5^2 = 60$, d'où il résulte facilement que $d_1 = d_2 = 3$.

La matrice des caractères de $\mathfrak{A}_5$ est de la forme $U = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 0 & 1 & -1 & -1 \\ 5 & 1 & -1 & 0 & 0 \\ 3 & a & b & c & d \\ 3 & a' & b' & c' & d' \end{pmatrix}$.

En utilisant la formule d'orthogonalité des colonnes (C.12 en annexe), on trouve, après un petit calcul (les deux dernières lignes sont bien sûr obtenues à permutation près) :

$$U = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 0 & 1 & -1 & -1 \\ 5 & 1 & -1 & 0 & 0 \\ 3 & -1 & 0 & \dfrac{\sqrt{5}+1}{2} & \dfrac{-\sqrt{5}+1}{2} \\ 3 & -1 & 0 & \dfrac{-\sqrt{5}+1}{2} & \dfrac{\sqrt{5}+1}{2} \end{pmatrix}.$$

On a donc deux représentations χ et $\check{\chi}$ de degré 3, dont les caractères sont réels. Faisons le point sur la table des caractères de $\mathfrak{A}_5$.

nom classe	1	2	3	5_1	5_2
1	1	1	1	1	1
ϕ	4	0	1	-1	-1
θ	5	1	-1	0	0
χ	3	-1	0	$\dfrac{\sqrt{5}+1}{2}$	$\dfrac{-\sqrt{5}+1}{2}$
$\check{\chi}$	3	-1	0	$\dfrac{-\sqrt{5}+1}{2}$	$\dfrac{\sqrt{5}+1}{2}$

Il s'agit maintenant de prouver que ces caractères de degré 3 se réalisent sur $\mathbb{R}$, au sens de E.3.

2.2. Première preuve de la réalisation sur $\mathbb{R}$ des caractères de degré 3 (abstraite)

En appliquant le critère de la proposition E.5, on vérifie que χ et $\check{\chi}$ peuvent se réaliser sur $\mathbb{R}$. En effet, on calcule

$$\frac{1}{|\mathfrak{A}_5|}\sum_{g\in\mathfrak{A}_5}\chi(g^2)=\frac{1}{60}\Big(3+15\times 3+20\times 0+12\times\frac{\sqrt{5}+1}{2}+12\times\frac{-\sqrt{5}+1}{2}\Big)=1.$$

Le calcul pour $\check{\chi}$ est identique par commutativité de l'addition.

Il existe donc un morphisme non trivial $\mathfrak{A}_5\to \mathrm{GL}_3(\mathbb{R})$, donc un morphisme non trivial $\mathfrak{A}_5\to \mathrm{O}_3(\mathbb{R})$ qui, comme $\mathfrak{A}_5$ est égal à son groupe dérivé, est à valeurs dans $\mathrm{SO}_3(\mathbb{R})$.

Exercice. *Montrer, sans utiliser la table de caractères, qu'il y a à isomorphisme près au plus deux représentations fidèles irréductibles de* $\mathfrak{A}_5$ *à valeurs dans* $\mathrm{SO}_3(\mathbb{R})$.

Par injectivité, un produit de deux transpositions est nécessairement envoyé sur un demi-tour (trace : -1), un 3-cycle sur une rotation d'angle $\pm 2\pi/3$ (trace : $1+2\cos 2\pi/3$), un 5-cycle sur une rotation d'angle $\pm 2\pi/5$ (trace : $1+2\cos 2\pi/5$) ou $\pm 4\pi/5$ (trace : $1+2\cos 4\pi/5$).

2.3. Deuxième preuve de la réalisation sur $\mathbb{R}$ des caractères de degré 3 (alternée)

Reprenons la représentation réelle[2] de permutation de $\mathfrak{A}_5$ provenant de l'action sur $X=\{1,2,3,4,5\}$. On a déjà calculé, à l'aide du nombre de points fixes, le caractère ϕ de la représentation irréductible correspondante :

nom classe	1	2	3	5_1	5_2
ϕ	4	0	1	-1	-1

Comme au paragraphe B.20, formons le carré alterné de ρ : c'est une représentation (réelle, par la remarque B.22) de degré $4\times(4-1)/2=6$, dont on calcule le caractère Λ par la proposition B.21 :

nom classe	1	2	3	5_1	5_2
Λ	6	-2	0	1	1

[2]Comme c'est une représentation provenant d'une action, on peut la réaliser sur n'importe quel corps.

On calcule la longueur de Λ : $\langle \Lambda, \Lambda \rangle = 2$. Comme la décomposition de 2 en somme de carrés est unique : $2 = 1^2 + 1^2$, on déduit que Λ est la somme de deux caractères irréductibles, voir l'exercice B.11 en annexe. On sait lesquels grâce à la table des caractères de $\mathfrak{A}_5$: $\langle \Lambda, \chi \rangle = 1 = \langle \Lambda, \check{\chi} \rangle$. Cela prouve que la représentation de caractère χ est une sous-représentation de $\bigwedge^2 \rho$, et qu'elle se réalise donc sur $\mathbb{R}$. On conclut comme lors de la première preuve qu'elle se réalise comme une représentation à valeurs dans le groupe $\mathrm{SO}_3(\mathbb{R})$.

Exercice. *Montrer que la représentation $\bigwedge^2 \rho$ de degré 6 de $\mathfrak{A}_5$ est la restriction d'une représentation irréductible de $\mathfrak{S}_5$.*

Considérer la représentation irréductible V_X associée à l'action naturelle de $\mathfrak{S}_5$ sur $X = \{1, 2, 3, 4, 5\}$. Calculer le caractère de son carré alterné, puis montrer que sa longueur est 1.

Exercice

1. *Décrire l'action du groupe de Galois de $\mathbb{C}$ sur $\mathbb{Q}$ sur $\mathrm{Irr}(\mathfrak{A}_5)$ définie dans l'exercice F.23.*
2. *Montrer que la transposition (12) de $\mathfrak{S}_5$ induit un automorphisme extérieur σ de $\mathfrak{A}_5$ qui permute ses deux classes de 5-cycles.*
3. *En déduire une description de l'action du groupe $\mathrm{Out}(\mathfrak{A}_5)$ sur $\mathrm{Irr}(\mathfrak{A}_5)$ définie dans l'exercice F.24.*

2.4. Troisième preuve de la réalisation sur $\mathbb{R}$ des caractères de degré 3 (tensorielle)

Reprenons le caractère ϕ de degré 4 :

nom classe	1	2	3	5_1	5_2
ϕ	4	0	1	-1	-1

Comme il provient d'une représentation par permutation, ce caractère peut se réaliser sur $\mathbb{R}$ (lemme E.2). Anticipant sur la remarque XI-A.6-3, son carré ϕ^2 est le caractère d'une représentation réelle V de degré 16. Or, on peut vérifier que ϕ^2 est la somme de toutes les représentations irréductibles de $\mathfrak{A}_5$:

$$\phi^2 = 1 + \phi + \psi + \chi + \check{\chi}.$$

En effet, on le vérifie directement ou bien on calcule (c'est plus long mais plus naturel pour décomposer ϕ^2) : $\langle \phi^2, 1 \rangle = \langle \phi^2, \phi \rangle = \langle \phi^2, \psi \rangle = \langle \phi^2, \chi \rangle = \langle \phi^2, \check{\chi} \rangle = 1$.

Ainsi, toutes les représentations de $\mathfrak{A}_5$ se réalisent sur $\mathbb{R}$ comme des sous-représentations de V.

2.5. Réalisation effective des représentations de degré 3

Étant donné un groupe fini, il est beaucoup plus difficile de construire ses représentations, c'est-à-dire les matrices, que de construire sa table des caractères, c'est-à-dire calculer leurs traces. La situation présente est significative : nous venons de prouver (trois fois même) qu'il existe une représentation $\mathfrak{A}_5 \to SO_3(\mathbb{R})$.

La ligne de χ dans la table des caractères apporte des informations, théoriques (à isomorphisme près), mais apporte-t-elle des informations effectives ? Franchement, pensez-vous que les cinq données de la ligne de χ vont permettre de reconstruire soixante matrices 3×3 ? Même en invoquant la formule magique de Marraine, la bonne fée de Cendrillon[3], on changera peut-être une citrouille en carrosse, mais l'on ne verra certainement pas apparaître nos matrices.

Nous allons donc voir ici que la construction des matrices est possible, mais n'est pas une chose facile. Voici une stratégie que l'on peut mettre en place sur un logiciel de calcul formel, comme SAGE[4] :

1. avoir un contrôle sur les éléments de $\mathfrak{A}_5$ et leurs classes de conjugaison ;
2. construire une représentation σ de degré 6 sur $\mathbb{R}$, et de caractère $\Lambda = \chi + \check{\chi}$, c'est-à-dire les matrices $\sigma(g)$ $(g \in \mathfrak{A}_5)$;
3. décomposer σ en irréductibles sur $\mathbb{R}$ ou sur $\mathbb{Q}(\sqrt{5})$ — c'est pareil ;
4. profiter de la vue !

Voici quelques précisions.

Énumération des éléments et des classes de conjugaison de $\mathfrak{A}_5$

Il faut commencer par énumérer les permutations de $\mathfrak{S}_5$, par exemple sous forme de listes. Précisons : la liste `[1,4,3,5,2]` représente le 3-cycle (245). Si ce n'est pas une primitive du logiciel utilisé, une façon de procéder consiste à partir de la liste à un élément `[1]` et à ajouter le chiffre 2 à tous les endroits possibles pour former les listes `[1,2]` et `[2,1]`, puis 3 à tous les endroits possibles, etc.

Puis, il s'agit de sélectionner les permutations paires. Si la signature d'une permutation codée par une liste `L` n'est pas implémentée, on peut la calculer par un produit de `(L[i]-L[j])/(i-j)`. (Ce n'est pas optimal mais bon, on travaille sur $\mathfrak{S}_5$.)

Puis, il s'agit de distinguer les deux classes de conjugaison de 5-cycles. Une façon de procéder consiste à conjuguer un 5-cycle $(1abcd)$ en $(123xy)$ par une permutation α (telle que $\alpha(a) = 2$, $\alpha(b) = 3$) et à distinguer selon que $xy = 45$ ou que $xy = 54$.

---

[3] *Salagadou, Lamenchikabou, Labibidi Bobidi Bou !*

[4] Le site officiel de cette plate-forme *libre* est `http://sagemath.org/`.

À ce stade, on doit disposer d'une liste des soixante permutations paires et d'une façon de leur associer leur classe de conjugaison.

Construction d'une « grosse » représentation

La stratégie est donc ici de construire une représentation réelle σ de degré 6. On sait le faire en prenant le carré alterné de la représentation irréductible de degré 4. Il s'agit de construire les matrices de la représentation irréductible V_X de degré 4 de $\mathfrak{A}_5$. Par définition de V_X, on peut construire les matrices de permutation puis faire un changement de base vers la base

$$(e_1 - e_5, e_2 - e_5, e_3 - e_5, e_4 - e_5, e_1 + e_2 + e_3 + e_4 + e_5),$$

et ne conserver que le bloc 4×4 supérieur gauche. Par exemple, les matrices correspondant à (12)(34) et (12345) sont :

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} -1 & -1 & -1 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Puis, il faut construire σ, le carré alterné de la représentation précédente, par exemple à l'aide de la remarque B.22. Il faut s'attendre à manipuler bon nombre d'indices... On trouve, pour $\sigma\big((12)(34)\big)$ et $\sigma\big((12345)\big)$:

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

À ce stade, on doit disposer d'une liste de soixante matrices 6×6 qui réalisent la représentation σ de caractère $\chi + \check{\chi}$ de $\mathfrak{A}_5$. Il est intéressant de remarquer qu'elles sont toutes à coefficients rationnels (et même entiers à vrai dire).

Remarque. Plutôt que travailler avec une base non canonique, on peut aussi choisir de rester en dimension 5 et d'appliquer aux matrices le projecteur sur la composante irréductible de degré 4, à savoir $\mathrm{I}_5 - J/5$, où J est la matrice n'ayant que des 1 (pourquoi est-ce bien le projecteur ?). On ne travaille plus vraiment avec des représentations du groupe, mais de l'*algèbre du groupe* $\mathbb{Q}[\mathfrak{A}_5]$.

Dans le même esprit, on peut se contenter de calculer le carré tensoriel plutôt que le carré alterné (moins d'indices). Le tout est d'avoir les matrices d'une représentation où interviennent une fois et une seule χ et $\check{\chi}$.

Première construction du projecteur, par moyenne sur le groupe

Une première méthode pour séparer les représentations de caractères χ et $\check{\chi}$ consiste à utiliser le projecteur sur la composante isotypique χ, c'est-à-dire :

$$P = \frac{\chi(1)}{|\mathfrak{A}_5|} \sum_{g \in \mathfrak{A}_5} \overline{\chi(g)}\, \sigma(g) = \frac{\chi(1)}{|\mathfrak{A}_5|} \sum_{g \in \mathfrak{A}_5} \chi(g)\, \sigma(g).$$

On trouve :

$$P = \frac{1}{2\sqrt{5}} \begin{pmatrix} \sqrt{5} & 1 & -1 & 1 & -1 & -3 \\ -1 & \sqrt{5} & 1 & 1 & 3 & 1 \\ 1 & -1 & \sqrt{5} & -3 & -1 & 1 \\ -1 & -1 & -3 & \sqrt{5} & -1 & -1 \\ 1 & 3 & 1 & 1 & \sqrt{5} & -1 \\ -3 & -1 & -1 & 1 & 1 & \sqrt{5} \end{pmatrix}.$$

Alors, P est un projecteur qui commute à $\mathfrak{A}_5$, dont l'image est la sous-représentation de dimension $\mathrm{tr}(P) = 3$ cherchée. En remplaçant χ par $\check{\chi}$ (ou P par $\check{P} = \mathrm{I}_6 - P$), on réalise la représentation de caractère $\check{\chi}$.

Cette méthode a l'avantage d'être générale et d'utiliser la belle et séduisante théorie des caractères. Mais l'inconvénient, c'est que l'on a vraiment besoin de toutes les matrices $\sigma(g)$.

Deuxième construction du projecteur, par les endomorphismes

On sait que la dimension de l'algèbre des endomorphismes qui commutent aux $\sigma(g)$ ($g \in \mathfrak{A}_5$) se calcule par le carré scalaire du caractère Λ de σ. On trouve comme prévu : $\langle \Lambda, \Lambda \rangle = 2$. On calcule directement le commutant de la représentation. Pour cela, il suffit d'écrire la commutation avec un ensemble de générateurs de $\mathfrak{A}_5$, par exemple (12)(34) et (12345). Cela revient à résoudre un système à trente-six inconnues et soixante-douze équations, l'aide d'un ordinateur étant agréable. On trouve une algèbre de dimension 2, dont une base est (I_6, E), où

$$E = \begin{pmatrix} 0 & 1 & -1 & 1 & -1 & -3 \\ -1 & 0 & 1 & 1 & 3 & 1 \\ 1 & -1 & 0 & -3 & -1 & 1 \\ -1 & -1 & -3 & 0 & -1 & -1 \\ 1 & 3 & 1 & 1 & 0 & -1 \\ -3 & -1 & -1 & 1 & 1 & 0 \end{pmatrix},$$

et l'on a :

$$E^2 = 5\mathrm{I}_6.$$

Au passage, on en déduit que la représentation de caractère Λ de $\mathfrak{A}_5$ est irréductible sur $\mathbb{Q}$. En effet, si elle se décomposait, il y aurait un projecteur non trivial compatible avec cette décomposition et donc une matrice à coefficients dans $\mathbb{Q}$ qui commute avec $\sigma\big((12)(34)\big)$ et $\sigma\big((12345)\big)$. Or, le

commutant est engendré par la matrice E telle que $E^2 = 5\mathrm{I}_6$, de sorte qu'un élément de la forme $P = \alpha \mathrm{I}_6 + \beta E$ ($\alpha, \beta \in \mathbb{Q}$) ne peut satisfaire à $P^2 = P$ que si $P = \mathrm{I}_6$. En revanche, on trouve des solutions α, β dans $\mathbb{Q}(\sqrt{5})$ (donc, *a fortiori*, sur $\mathbb{R}$). Les projecteurs sur ces sous-représentations sont (oui, c'est le même P que ci-dessus, et $\check{P} = \mathrm{I}_6 - P$) :

$$P = \frac{1}{2\sqrt{5}}(E + \sqrt{5}\,\mathrm{Id}) \quad \text{et} \quad \check{P} = -\frac{1}{2\sqrt{5}}(E - \sqrt{5}\,\mathrm{Id}).$$

Matrice des représentations de degré 3

Pour g de $\mathfrak{A}_5$, la matrice $\sigma(g)$ agit comme la représentation de caractère χ (resp. $\check{\chi}$) sur $\mathrm{im}(P)$ (resp. $\ker(P)$). Si l'on trouve une base de $\mathrm{im}(P)$ et de $\ker(P)$, qui est aussi égal à $\mathrm{im}(\check{P})$, après changement de base, les $\sigma(g)$ deviendront diagonales par blocs 3×3.

On pourrait choisir n'importe quelle base. Mais, il est commode qu'elle soit orthonormée et adaptée à $\mathfrak{A}_5$. On se rappelle que les 2-Sylow de $\mathfrak{A}_5$ sont isomorphes au groupe de Klein et que deux demi-tours qui commutent dans $\mathrm{SO}_3(\mathbb{R})$ ont des axes orthogonaux : cela assure en particulier que les axes sont linéairement indépendants. On choisit un 2-Sylow $\{\mathrm{Id}, g_1, g_2, g_3\}$, disons celui qui contient $g_1 = (12)(34)$ et une base $(v_1, v_2, v_3, \check{v}_1, \check{v}_2, \check{v}_3)$ de sorte que v_i (resp. $\check{v}_i$) engendre l'axe de $P\sigma(g_i)$ (resp. $\check{P}\sigma(g_i)$). On trouve pour matrice de passage :

$$Q = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & \frac{\sqrt{5}-3}{2} & 1 & 0 & \frac{-\sqrt{5}-3}{2} \\ \frac{\sqrt{5}-3}{2} & \frac{-\sqrt{5}-3}{2} & 0 & \frac{-\sqrt{5}-3}{2} & \frac{\sqrt{5}-3}{2} & 0 \\ \frac{\sqrt{5}-3}{2} & \frac{\sqrt{5}+3}{2} & 0 & \frac{-\sqrt{5}-3}{2} & \frac{-\sqrt{5}+3}{2} & 0 \\ 1 & 0 & \frac{-\sqrt{5}+3}{2} & 1 & 0 & \frac{\sqrt{5}+3}{2} \\ 0 & 1 & -1 & 0 & 1 & -1 \end{pmatrix}.$$

Les trois premiers vecteurs et les trois derniers vecteurs sont bien orthogonaux, mais la base n'est pas normée :

$$\|v_1\|^2 = 9 - 3\sqrt{5} = \|v_3\|^2, \quad \|v_2\|^2 = 9 + 3\sqrt{5}.$$

Pour y remédier, il est commode de vérifier que $(9 + 3\sqrt{5})/(9 - 3\sqrt{5}) = (3+\sqrt{5})^2/4$. Cela incite à remplacer v_2 par $v_2' = 2/(3+\sqrt{5})\, v_2$, de sorte que la base (v_1, v_2', v_3) soit orthogonale et que ses vecteurs aient tous la même norme. Il n'y a plus qu'à écrire les matrices dans cette base. On trouve par

exemple :

$$(12)(34) : \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad (12345) : \begin{pmatrix} \frac{\sqrt{5}+1}{4} & \frac{\sqrt{5}-1}{4} & -\frac{1}{2} \\ \frac{\sqrt{5}-1}{4} & \frac{1}{2} & \frac{\sqrt{5}+1}{4} \\ \frac{1}{2} & -\frac{\sqrt{5}+1}{4} & \frac{\sqrt{5}-1}{4} \end{pmatrix}.$$

Pour les sommets de l'icosaèdre, il suffit de trouver des vecteurs fixes de même norme pour tous les 5-cycles. Ou bien, d'en choisir un et de faire agir le groupe $\mathfrak{A}_5$. Par exemple, la matrice de (12345) ci-dessus fixe le vecteur $((\sqrt{5}+1)/2, 1, 0)$ ce qui permet de deviner (ou retrouver...) les coordonnées des autres sommets : changer les signes arbitrairement et permuter cycliquement les coordonnées.

Pour les sommets d'un dodécaèdre, on partira d'un vecteur fixé par un élément d'ordre 3.

Bonus : la 600-cellule !

À ce stade, on dispose en principe d'une liste (voire deux) de soixante matrices orthogonales 3×3 à coefficients dans $\mathbb{Q}(\sqrt{5})$ qui réalisent une représentation de degré 3 de $\mathfrak{A}_5$. Il ne coûte pas très cher de programmer la recherche explicite des antécédents d'une matrice par la projection $\varpi : SU_2(\mathbb{C}) \to SO_3(\mathbb{C})$. Par [H2G2, chapitre VII], on sait que $SU_2(\mathbb{C})$ peut être réalisé comme la sphère $\mathbf{S}^3$ des quaternions et, à ce titre, engendre un sous-espace de dimension 4 sur $\mathbb{R}$ dans $\mathscr{M}_2(\mathbb{C})$ — la réalisation matricielle complexe de l'espace des quaternions. Les cent-vingt matrices obtenues se trouvent être les sommets d'un polyèdre régulier de $\mathbb{R}^4 \subset \mathscr{M}_2(\mathbb{C})$. On peut en déterminer les arêtes : segments ou arcs de sphère reliant les sommets à distance minimale non nulle. Ce polyèdre possède des « faces » de dimension 3, appelées *cellules*. Elles sont toutes tétraédriques et sont au nombre de 600. On peut représenter le polyèdre par une perspective cavalière (voir, par exemple, `http://en.wikipedia.org/wiki/600-cell`) ou bien, comme il est inclus dans la sphère-unité de dimension 3, par une projection stéréographique (voir le chapitre 4 du film *Dimensions* [2] d'Aurélien Alvarez, Étienne Ghys et Jos Leys).

A. Annexe. Théorie des représentations

L'idée maîtresse de la théorie, c'est qu'une représentation est une « réalisation » du groupe sur laquelle on peut faire des calculs, et que l'étude de toutes les représentations donne des renseignements précieux sur le groupe, ainsi que sur ses actions. Une idée un peu plus vague mais extrêmement générale se résume en un mot : la *linéarisation*. Ici, il s'agit de plonger un groupe (ou un quotient du groupe) dans un groupe de matrices.

Le succès le plus spectaculaire de la théorie, c'est la classification des groupes finis simples, dans laquelle une étape importante est le théorème très difficile suivant, dû à Feit et Thompson : *tout groupe fini de cardinal impair est résoluble*. L'hypothèse est de nature « géométrique » (la géométrie sur les ensemble finis, ce sont les cardinaux, comme on l'a vu dans [H2G2, chapitre VII]), la conclusion est de nature algébrique et, pour la preuve, la théorie des représentations est indispensable. Burnside avait, dès les débuts de la théorie, démontré un énoncé dont la structure est analogue mais beaucoup plus facile : tout groupe fini dont le cardinal n'a que deux diviseurs premiers est résoluble.

Cette annexe est, pour parler par euphémismes, fortement inspirée par le livre de Jean-Pierre Serre [76]. On y trouve en plus quelques digressions dilatoires et peut-être quelques erreurs.

Dans toute les annexes, on fixe un groupe fini G, dont on note e le neutre, et un corps $\mathbb{K}$.

A.1. Définition. Une *représentation linéaire* ou plus simplement une *représentation* de G est la donnée d'un espace vectoriel V sur $\mathbb{K}$, disons de dimension finie, et d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$. Par abus, on dit parfois que V est une représentation, ou un G-module, si le morphisme ρ est sous-entendu. On dit aussi que $\rho : G \to \mathrm{GL}(V)$ est une représentation. Une représentation sera dite *fidèle* si ρ est injective. Le *degré* d'une représentation V est la dimension de V.

Une *sous-représentation* de V est (la restriction de ρ à) un sous-espace vectoriel stable par $\rho(g)$ pour tout g de G. Une représentation est *irréductible* ou *simple* si elle n'est pas réduite à $\{0\}$ et si elle n'admet pas de sous-représentation autre que $\{0\}$ et V.

Si $\rho : G \to \mathrm{GL}(V)$ et $\rho' : G \to \mathrm{GL}(V')$ sont deux représentations, un *morphisme de représentations* ou *opérateur d'entrelacement* de V vers V' est une application linéaire $\varphi : V \to V'$ telle que :

$$\forall g \in G, \quad \varphi \circ \rho(g) = \rho'(g) \circ \varphi.$$

On dit que ρ et ρ' (ou V et V' s'il n'y a pas d'ambiguïté possible) sont des représentations *isomorphes* ou *équivalentes* s'il existe un opérateur d'entrelacement inversible de V vers V'.

Exemple. Prenons $V = \mathbb{K}$ et $\rho_{\mathrm{triv}} : G \to \mathrm{GL}(V) = \mathbb{K}^*$, $g \mapsto 1$: c'est la représentation *triviale*, elle est de degré 1.

Il existe une autre représentation que l'on sait définir pour tout groupe (fini) G, il s'agit de la représentation régulière. On la retrouvera tout le long de cette annexe.

Exemple. La *représentation régulière* de G est définie ainsi. L'espace ambiant est le $\mathbb{C}$-espace $\mathbb{C}G$, qui a pour base $(\delta_g)_{g\in G}$. L'action d'un élément g de G est définie par :

$$\forall h \in G, \quad \rho_{\mathrm{reg}}(g)(\delta_h) = \delta_{gh}.$$

Une représentation n'est rien d'autre qu'une *action linéaire* de G sur V, c'est-à-dire une action $\alpha : G \times V \to V$ telle que pour tout g de G, l'application $\rho(g) : V \to V$, $v \mapsto \alpha(g, v)$ soit linéaire.

Si $\rho : G \to \mathrm{GL}(V)$ est une représentation de degré n, le choix d'une base de V induit un morphisme de G dans $\mathrm{GL}_n(\mathbb{K})$. Inversement, si l'on identifie $\mathrm{GL}_n(\mathbb{K})$ à $\mathrm{GL}(\mathbb{K}^n)$, un morphisme $G \to \mathrm{GL}_n(\mathbb{K})$ est une représentation, que l'on peut appeler *matricielle.*

La composée de deux morphismes de représentations, si elle est définie, est encore un morphisme de représentations ; de même, si un morphisme de représentations est un isomorphisme, son inverse est encore un morphisme de représentations. Il en résulte que l'équivalence de représentations est bien une relation d'équivalence. Quel soulagement !

Exemple. Soit n un entier naturel non nul, soit $G = \mathbb{Z}/n\mathbb{Z}$ et soit g un générateur de G. Une représentation de G est déterminée par l'automorphisme $\sigma = \rho(g)$, car on impose, pour k entier : $\rho(g^k) = \rho(g)^k$. Il est nécessaire (évidemment) et suffisant (par passage au quotient) d'imposer la relation : $\sigma^n = \mathrm{Id}_V$. Ainsi, une représentation de $\mathbb{Z}/n\mathbb{Z}$ est déterminée par un espace V et un automorphisme σ de V d'ordre divisant n.

A.2. La fabrique des représentations

À partir de deux représentations $\rho : G \to \mathrm{GL}(V)$ et $\sigma : G \to \mathrm{GL}(W)$, on en fabrique d'autres :

(a) sur la somme directe $V \oplus W = V \times W$, on fait agir un élément g de G par la somme directe de $\rho(g)$ et $\sigma(g)$:

$$\forall (v, w) \in V \times W, \quad (\rho \oplus \sigma)(g)(v, w) = \big(\rho(g)(v), \sigma(g)(w)\big) ;$$

autrement dit, la matrice de la somme directe de deux représentations ρ et σ est composée par blocs diagonaux des matrices de ρ et de σ ;

(b) sur le dual V^*, on fait agir g sur V^* par la transposée de son inverse[5], d'où une représentation $\check{\rho} : G \to \mathrm{GL}(V^*)$:

$$\forall \ell \in V^*,\ \forall v \in V,\quad \big(\check{\rho}(g)(\ell)\big)(v) = \big({}^t\rho(g)^{-1}(\ell)\big)(v) = \ell\big(\rho(g^{-1})(v)\big)\,;$$

(c) sur l'espace $\mathrm{Hom}_{\mathbb{K}}(V,W)$, on fait agir un élément g de G ainsi :

$$\forall \varphi \in \mathrm{Hom}_{\mathbb{K}}(V,W),\quad g\cdot\varphi = \sigma(g)\circ\varphi\circ\rho(g^{-1})\,;$$

(d) si W est une sous-représentation de V, on note $\overline{v}$ la classe d'un vecteur v de V dans le quotient V/W ; on vérifie que l'on définit une nouvelle représentation $\bar{\rho}$ en posant, pour $g \in G$ et $v \in V$: $g\cdot\overline{v} = \overline{\rho(g)(v)}$ (de sorte que la projection naturelle $V \to V/W$ est un morphisme de représentations) ; on l'appelle *représentation-quotient* (eh !) ;

(e) sur l'espace $\mathrm{Bil}(V)$ des formes bilinéaires sur V, on fait agir G par congruence : pour β dans $\mathrm{Bil}(V)$ et g dans G, on définit[6] :

$$\forall u,v \in V,\quad (g\cdot\beta)(u,v) = \beta\big(\rho(g^{-1})u, \rho(g^{-1}v)\big);$$

les formes bilinéaires symétriques (resp. alternées) constituent des sous-représentations de $\mathrm{Bil}(V)$.

On pourra éventuellement sauter les deux exercices suivants en première lecture.

A.3. Exercice. *On a vu, en [H2G2, définition V-A.1.1], l'isomorphisme linéaire qui, à β dans* $\mathrm{Bil}(V)$, *associe $\psi_\beta \in \mathrm{Hom}(V,V^*)$, défini par :*

$$\forall v,w \in V,\quad \psi_\beta(v)(w) = \beta(v,w).$$

Montrer que pour les actions de G définies ci-dessus sur V^*, $\mathrm{Hom}(V,V^*)$ *et* $\mathrm{Bil}(V)$, *l'isomorphisme $\beta \mapsto \psi_\beta$, établit un isomorphisme de G-modules entre* $\mathrm{Bil}(V)$ *et* $\mathrm{Hom}(V,V^*)$.

On a d'une part :

$$\psi_{g\cdot\beta}(v)(w) = (g\cdot\beta)(v,w) = \beta\big(\rho(g)^{-1}(v), \rho(g)^{-1}(w)\big),$$

et d'autre part :

$$\begin{aligned}(g\cdot\psi_\beta)(v)(w) &= {}^t\rho(g)^{-1}\Big(\psi_\beta\big(\rho(g)^{-1}(v)\big)\Big)(w)\\ &= \psi_\beta\big(\rho(g)^{-1}(v)\big)\big(\rho(g)^{-1}(w)\big)\\ &= \beta\big(\rho(g)^{-1}(v), \rho(g)^{-1}(w)\big).\end{aligned}$$

[5]Comme maintes autres fois, l'inverse est là pour assurer que l'on obtienne un morphisme et pas un anti-morphisme de G vers $\mathrm{GL}(V^*)$.

[6]Les inverses sont nécessaires pour avoir une action à gauche, et l'on vérifie que l'action est bien linéaire.

A.4. Exercice. *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation. Si $\mathbf{e} = (e_1, \ldots, e_n)$ une base fixée de V, on note $\mathbf{e}^*$ sa base duale. Pour tout élément g de G, on note $\rho_0(G) \in \mathrm{GL}_n(\mathbb{K})$ la matrice de $\rho(g)$ dans $\mathbf{e}$. On dit que ρ_0 est la* représentation matricielle *associée à V (et $\mathbf{e}$).*

1. *Vérifier que deux représentations ayant les mêmes matrices sont isomorphes.*
2. *Soit g dans G. Montrer que la matrice $\check{\rho}(g)$ dans la base $\mathbf{e}^*$ est ${}^t\rho_0(g)^{-1}$.*
3. *Soit k un entier compris entre 1 et n. On suppose que l'espace W engendré par les k vecteurs $e_1, \ldots, e_k$ est une sous-représentation. Montrer que pour tout g de G, la matrice $\rho_0(g)$ est de la forme*

$$\begin{pmatrix} \sigma_0(g) & B(g) \\ 0 & \bar{\rho}_0(g) \end{pmatrix},$$

où $\sigma_0(g)$ est la matrice de g dans la base $(e_1, \ldots, e_k)$ et $\bar{\rho}_0(g)$ est la matrice de $\bar{\rho}(g)$ dans la base image de $(\overline{e_{k+1}}, \ldots, \overline{e_n})$ de V/W. (Comparer à l'exercice II-A.5.)

4. *Soit β une forme bilinéaire sur l'espace V et soit B sa matrice dans $\mathbf{e}$. Avec les notations de l'alinéa* (e) *ci-dessus, montrer que la matrice de la forme bilinéaire $g \cdot \beta$ est : ${}^t\rho_0(g)^{-1} B \rho_0(g)^{-1}$.*

   C'est la formule habituelle de la congruence ! Réponse p. B.18.

A.5. Invariants et morphismes de représentations

Dans V, le sous-espace[7]

$$V^G = \{v \in V,\ \forall g \in G,\ \rho(g)(v) = v\}$$

est une sous-représentation appelée *espace des invariants* de V ; elle est isomorphe à $\dim(V^G)$ copies $\rho_{\mathrm{triv}} \oplus \cdots \oplus \rho_{\mathrm{triv}}$ de la représentation triviale.

Cela s'applique en particulier à l'espace des invariants de $\mathrm{Hom}_{\mathbb{K}}(V, W)$ (pour l'action de G définie plus haut), noté $\mathrm{Hom}_{\mathbb{K}}(V, W)^G$. Si φ est un morphisme de $\mathrm{Hom}_{\mathbb{K}}(V, W)^G$, alors, $\rho_W(g^{-1}) \circ \varphi \circ \rho_V(g) = \varphi$, ce qui est équivalent à $\varphi \circ \rho_V(g) = \rho_W(g) \circ \varphi$. Et donc, l'espace $\mathrm{Hom}_{\mathbb{K}}(V, W)^G$ est égal à l'espace $\mathrm{Hom}_{\mathbb{K}G}(V, W)$ des morphismes de représentations.

A.6. Proposition. *Soit G un groupe et soient V et W deux représentations de G. Pour l'action linéaire de G définie plus haut sur $\mathrm{Hom}_{\mathbb{K}}(V, W)$, le sous-espace vectoriel des invariants $\mathrm{Hom}_{\mathbb{K}}(V, W)^G$ est égal au sous-espace $\mathrm{Hom}_{\mathbb{K}G}(V, W)$ des morphismes de représentations de V vers W.*

En particulier, la sous-algèbre des invariants $\mathrm{End}_{\mathbb{K}}(V)^G$ est égale à la sous-algèbre $\mathrm{End}_{\mathbb{K}G}(V)$ des endomorphismes de la représentation V.

[7] On peut le voir comme l'intersection des espaces propres $\ker(\rho(g) - \mathrm{Id}_V)$.

Une homothétie est un morphisme de représentations, si bien que l'espace des morphismes d'une représentation V dans elle-même est une sous-algèbre unitaire de $\mathrm{End}_{\mathbb{K}}(V)$, notée $\mathrm{End}_{\mathbb{K}G}(V)$ ou $\mathrm{End}_{\mathbb{K}}(V)^G$ (voir l'exercice qui suit) ; on l'appelle parfois *commutant* de V.

A.7. Exercice. *Montrer que le sous-espace des invariants d'une somme directe est la somme directe des sous-espaces des invariants : si V et W sont deux représentations, on a ainsi $(V \oplus W)^G = V^G \oplus W^G$.*

Lemme de Schur

Le *lemme de Schur* est un résultat dont l'ampleur des applications n'a d'égale que la simplicité de la preuve. Deux raisons pour bien le connaître !

A.8. Proposition (Lemme de Schur). *Soient $\rho : G \to \mathrm{GL}(V)$ et $\rho' : G \to \mathrm{GL}(V')$ deux représentations irréductibles et soit $\varphi : V \to V'$ un morphisme de représentations. Alors :*

(i) *le morphisme φ est nul ou bien c'est un isomorphisme ;*

(ii) *si $V = V'$ et $\mathbb{K}$ est algébriquement clos, alors φ est une homothétie.*

Démonstration. (i) La propriété de commutation $\varphi \circ \rho(g) = \rho'(g) \circ \varphi$, valable pour tout g de G, fait que le noyau et l'image de φ sont stables par G, c'est-à-dire que ce sont deux sous-représentations. Par irréductibilité de V et V', on peut affirmer que φ est nulle ou injective et qu'elle est nulle ou surjective. Par suite, elle est nulle ou bijective.

(ii) Si $\mathbb{K}$ est algébriquement clos, un élément φ de $\mathrm{End}_{\mathbb{K}G}(V)$ admet une valeur propre $\lambda \in \mathbb{K}$. Mais alors, $\ker(\varphi - \lambda \mathrm{Id}_V)$ est une sous-représentation de V non réduite à $\{0\}$. Il vient : $V = \ker(\varphi - \lambda \mathrm{Id}_V)$, d'où : $\varphi = \lambda \mathrm{Id}_V$. □

A.9. Corollaire. *L'algèbre des morphismes d'une représentation irréductible sur $\mathbb{K}$ est une algèbre à division (un corps non nécessairement commutatif) contenant $\mathbb{K} = \mathbb{K}\,\mathrm{Id}_V$; de plus, si $\mathbb{K}$ est algébriquement clos, alors c'est $\mathbb{K}\,\mathrm{Id}_V$.*

Démonstration. Pour la première partie de l'assertion, il suffit de prouver que l'inverse d'un morphisme de représentation, s'il existe, en est un également : cela résulte de la relation de commutation. L'assertion (ii) de la proposition donne l'inclusion de l'espace des invariants dans $\mathbb{K}\,\mathrm{Id}_V$, l'inclusion inverse étant claire. □

A.10. Remarque. Lorsque $\mathbb{K}$ n'est pas algébriquement clos, il peut arriver que les endomorphismes d'une représentation irréductible V forment un corps strictement plus gros que $\mathbb{K}$ et même que celui-ci ne soit pas commutatif. L'exercice F.9 donne un exemple.

On peut d'autre part poser la question de la réciproque : si l'algèbre des endomorphismes d'une représentation sur $\mathbb{K}$ est un corps (resp. est $\mathbb{K}$), est-ce que la représentation est irréductible ? En caractéristique zéro, oui : si V admet un sous-espace stable non trivial W, celui-ci admet un supplémentaire stable W' par le théorème de Maschke A.12 ci-dessous ; le projecteur sur W parallèlement à W' est un endomorphisme de la représentation V non nul et non inversible. En caractéristique p non nulle, en revanche, la réciproque est fausse : voir l'exercice F.13.

A.11. Semi-simplicité et invariants

On a suffisamment insisté là-dessus dans le tome premier : l'existence d'un supplémentaire est une propriété très importante des espaces vectoriels que l'on déduit du théorème de la base incomplète. Mais l'on sait bien qu'un sous-espace stable par un endomorphisme n'a pas nécessairement de supplémentaire stable. Par exemple, l'endomorphisme de $\mathbb{K}^2$ ayant pour matrice

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

dans la base canonique (e_1, e_2), possède un sous-espace stable $\mathbb{K}e_1$, mais celui-ci ne possède pas de supplémentaire stable. On s'intéresse fortement au théorème suivant, appelé *théorème de Maschke.*

A.12. Théorème (Maschke). *Supposons la caractéristique de $\mathbb{K}$ nulle ou égale à p premier avec $|G|$. Alors, toute sous-représentation possède un supplémentaire stable par G.*

A.13. Définition. On dit qu'une représentation de G est *semi-simple* si toute sous-représentation possède un supplémentaire stable par G.

En termes plus sophistiqués, on dit que l'algèbre $\mathbb{K}G$, définie au §D, est un anneau *semi-simple* sous l'hypothèse du théorème de Maschke. Le §A.15 et le §A.16 en donnent deux preuves : la première est spécifique au corps des complexes, la deuxième fonctionne pour tout corps satisfaisant à l'hypothèse du théorème. Le mot-clé des deux preuves est : *moyenner*[8]. Avant cela, un exemple permet de se convaincre que l'hypothèse sur la caractéristique est indispensable.

A.14. Exemple. Si p un nombre premier, on note $\mathbb{K} = \mathbb{F}_p$ le corps à p éléments. Soit par ailleurs G le groupe $\mathbb{Z}/p\mathbb{Z}$ et soit g un générateur de G. Soit enfin $V = \mathbb{F}_p^2$ la représentation sur laquelle g agit par la matrice $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, ce qui a un sens, car A^p est l'identité. Alors, le premier vecteur de la base

[8] De là à dire que la formation des professeurs est retournée au moyennage...

canonique engendre une droite stable (par g ou par G, cela revient au même), mais cette droite n'a pas de supplémentaire stable puisque A n'est pas diagonalisable.

A.15. Preuve de semi-simplicité, version 1 : sur $\mathbb{C}$

Dans ce court paragraphe, on suppose que le corps de base $\mathbb{K}$ est le corps des complexes. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation. On fixe une forme hermitienne définie positive $\langle \cdot, \cdot \rangle$ sur V et l'on en construit une nouvelle en posant :

$$\forall v, w \in V, \quad \langle v, w \rangle_G = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)(v), \rho(g)(w) \rangle.$$

La semi-simplicité de V résulte du lemme suivant.

Lemme. *La forme sesquilinéaire $\langle \cdot, \cdot \rangle_G$ est définie positive et invariante par le groupe G :*

$$\forall g \in G, \ \forall v, w \in V, \quad \big\langle \rho(g)(v), \rho(g)(w) \big\rangle_G = \langle v, w \rangle_G.$$

L'orthogonal d'une sous-représentation V' est une sous-représentation, et celle-ci est (bien sûr) supplémentaire à V'.

Démonstration. Pour v dans V, on a : $\langle v, v \rangle_G \geqslant 0$ puisque dans la somme qui définit $\langle v, v \rangle_G$ chaque terme $\langle \rho(g)v, \rho(g)v \rangle$ est positif ou nul. Pour qu'il y ait égalité, il faut que le terme correspondant à $g = e$ soit nul, si bien que $\langle v, v \rangle = 0$, ou encore : $v = 0$.

Pour vérifier l'invariance de $\langle \cdot, \cdot \rangle_G$, on fixe g, v et w :

$$\begin{aligned} \big\langle \rho(g)(v), \rho(g)(w) \big\rangle_G &= \frac{1}{|G|} \sum_{h \in G} \big\langle \rho(h)\rho(g)(v), \rho(h)\rho(g)(w) \big\rangle \\ &= \frac{1}{|G|} \sum_{h \in G} \big\langle \rho(hg)(v), \rho(hg)(w) \big\rangle = \langle v, w \rangle_G. \end{aligned}$$

Enfin, si V' est une sous-représentation de V et si v appartient à l'orthogonal $V'^{\perp}$ de V' pour $\langle \cdot, \cdot \rangle_G$, on a, pour tout $w \in V'$ et tout $g \in G$:

$$\big\langle \rho(g)v, w \big\rangle_G = \big\langle v, \rho(g^{-1})w \big\rangle_G = 0$$

puisque $\rho(g^{-1})w$ appartient à V'. Ainsi, $V'^{\perp}$ est invariant par G. □

A.16. Preuve de semi-simplicité, version 2

Soit $\rho : G \to \mathrm{GL}(V)$ une représentation et soit V' une sous-représentation de V. Fixons un projecteur p de V sur V', c'est-à-dire un endomorphisme

tel que : $p^2 = p$ et $\operatorname{im} p = V'$. On moyenne[9] :

$$p_G = \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ p \circ \rho(g)^{-1}.$$

On a alors :

$$\forall h \in G, \quad \rho(h) p_G \rho(h)^{-1} = \frac{1}{|G|} \sum_{g \in G} \rho(hg) \circ p \circ \rho(hg)^{-1} = p_G,$$

c'est-à-dire que p_G est un morphisme de G-modules[10]. En particulier, le noyau $\ker(p_G)$ de p_G est un sous-G-module de V.

Par ailleurs, l'image de p_G est incluse dans V' : pour tous g et v, $p\rho(g)(v)$ appartient à V', et V' est stable par $\rho(g)$.

Ensuite, si v appartient à V', alors, pour tout g, $\rho(g^{-1})(v)$ appartient à V' donc $p\rho(g^{-1})(v) = \rho(g^{-1})(v)$, d'où il résulte que : $p_G(v) = v$. En particulier, V' est inclus dans $\operatorname{im}(p_G)$, d'où l'égalité $V' = \operatorname{im}(p_G)$. De plus, p_G vaut l'identité sur son image, et donc $p_G \circ p_G = p_G$.

Ainsi, p_G est un projecteur et c'est un morphisme de G-modules dont l'image est V' : on en déduit que $\ker p_G$ est un supplémentaire de V' stable par G.

Décomposition en somme d'irréductibles

A.17. Notations. Soit $\mathbb{K}$ un corps dont la caractéristique est nulle ou première à $|G|$. On note $\mathrm{Irr}_{\mathbb{K}}(G)$ ou, plus simplement, $\mathrm{Irr}(G)$, si le corps est implicite, l'ensemble des classes d'isomorphismes de représentations irréductibles de G sur $\mathbb{K}$; pour $i \in \mathrm{Irr}(G)$, on choisit une fois pour toutes une représentation S_i dans la classe i.

A.18. Proposition. *Soit $\mathbb{K}$ un corps dont la caractéristique est nulle ou première à $|G|$. Soit V une représentation de G.*

(i) *On a :*

$$V \simeq \bigoplus_{i \in \mathrm{Irr}_{\mathbb{K}}(G)} S_i^{m_i/s_i},$$

où $m_i = \dim \mathrm{Hom}_{\mathbb{K}G}(S_i, V)$ et $s_i = \dim \mathrm{End}_{\mathbb{K}G}(S_i)$ pour tout i.

(ii) *Si $V \simeq \bigoplus_{i \in \mathrm{Irr}_{\mathbb{K}}(G)} S_i^{m'_i}$, alors on a : $m'_i = m_i/s_i$ pour tout i.*

(iii) *Pour tout i dans $\mathrm{Irr}(G)$, la composante de V correspondant à la sous-représentation $S_i^{m_i/s_i}$ est une sous-représentation canonique de V.*

[9] Cela revient à poser $p_G = \pi(p)$, où π est le projecteur de la proposition A.21 pour $W = \mathrm{End}_{\mathbb{K}}(V)$ pour la structure de G-module sur W, voir la proposition A.6.

[10] Vu que $p_G = \pi(p)$, cela résulte de la proposition A.21.

Remarque. Le calcul explicite de m_i, appelé *multiplicité* de la composante irréductible S_i dans V, se fait à l'aide des caractères. Tout cela sera précisé dans le corollaire B.9.

Démonstration. Montrons (i). On montre d'abord, par récurrence sur la dimension de V, que toute représentation V est somme directe de représentations irréductibles. En effet, si V est une droite, c'est une représentation irréductible. Soit n un entier supérieur ou égal à 2. On suppose que toute représentation de dimension au plus $n-1$ a une décomposition. Soit V une représentation de dimension n. Si V est irréductible, c'est terminé. Sinon, V possède une sous-représentation V' de dimension comprise entre 1 et $n-1$ et, par le théorème de Maschke, il existe une autre sous-représentation V'' telle que $V' \oplus V'' = V$. L'hypothèse de récurrence appliquée à V' et V'' permet de conclure.

À présent, on fixe une décomposition de $V = \bigoplus_{k=1}^{p} V_k$, où $V_1, \ldots, V_p$ sont des représentations irréductibles (distinctes ou non). Pour $i \in \mathrm{Irr}(G)$, on a :

$$\begin{aligned}\mathrm{Hom}_{\mathbb{K}G}(S_i, V) &= \Big(\mathrm{Hom}_{\mathbb{K}}(S_i, \bigoplus_{k=1}^{p} V_k)\Big)^G \\ &= \Big(\bigoplus_{k=1}^{p} \mathrm{Hom}_{\mathbb{K}}(S_i, V_k)\Big)^G \\ &= \bigoplus_{k=1}^{p} \mathrm{Hom}_{\mathbb{K}G}(S_i, V_k).\end{aligned}$$

La première et la troisième égalités proviennent de la proposition A.6, la deuxième est toujours valable avec un nombre fini de composantes.

Par la proposition A.8 (i), l'espace des morphismes de représentations de S_i dans V_k est de dimension s_i si V_k est isomorphe à S_i et 0 sinon. On en déduit que le nombre d'indices k tels que V_k est isomorphe à S_i est $s_i^{-1} \dim \mathrm{Hom}_{\mathbb{K}G}(S_i, V)$, ce qui entraîne les assertions (i) et (ii).

Enfin, l'assertion (iii) résulte aussi de l'égalité ci-dessus, puisque l'image de S_i par $\mathrm{Hom}_{\mathbb{K}G}(S_i, V)$, *i.e.* l'espace des $\sum_\varphi \varphi(S_i)$ où φ parcourt $\mathrm{Hom}_{\mathbb{K}G}(S_i, V)$, est donc la somme des V_k, où V_k est isomorphe à S_i et l'on a donc :

$$\mathrm{Hom}_{\mathbb{K}G}(S_i, V)(S_i) = S_i^{m_i/s_i}.$$

Comme le membre de gauche ne dépend pas de la décomposition de V choisie, l'assertion (iii) en découle. □

A.19. Définition. On garde les notations de la proposition A.18. Pour tout i dans $\mathrm{Irr}(G)$, la composante $S_i^{m_i/s_i}$ de V, qui ne dépend pas de la décomposition en irréductibles de V, est appelée *composante isotypique* de type i de V.

A.20. Exercice. *Soient deux représentations complexes V et V' admettant des décompositions $V \simeq \bigoplus_{i\in \mathrm{Irr}_{\mathbb{K}}(G)} S_i^{n_i}$ et $V' \simeq \bigoplus_{i\in \mathrm{Irr}_{\mathbb{K}}(G)} S_i^{n'_i}$, avec n_i et n'_i entiers. Montrer que l'on a :*

$$\dim \mathrm{Hom}_{\mathbb{K}G}(V,V') = \sum_{i\in \mathrm{Irr}_{\mathbb{K}}(G)} e_i n_i n'_i,$$

où $e_i = \dim_{\mathbb{K}} \mathrm{End}_{\mathbb{K}G}(S_i)$ pour tout i.

On choisit une décomposition de G-représentations

$$V = \bigoplus_{i\in \mathrm{Irr}(G)} \bigoplus_{1\leqslant k\leqslant n_i} S_{i,k} \quad \Big(\text{resp. } \quad V' = \bigoplus_{i\in \mathrm{Irr}(G)} \bigoplus_{1\leqslant k\leqslant n_i} S'_{i,k}\Big),$$

de sorte que $S_{i,k}$ (resp. $S'_{i,k}$) soit isomorphe à S_i, et une base $\mathbf{e}$ (resp. $\mathbf{e}'$) de V (resp. V') adaptée à cette décomposition. Décrire un élément de $\mathrm{Hom}_{\mathbb{K}G}(V,V')$ sous forme matricielle dans $\mathbf{e}$ et $\mathbf{e}'$.

Les matrices sont diagonales par blocs indexés par $\mathrm{Irr}(G)$; le bloc d'indice i est de taille $n'_i d_i \times n_i d_i$; il s'écrit lui-même par blocs de taille $d_i \times d_i$ de la forme $(\lambda_{k',k})$, où $1 \leqslant k \leqslant n_i$, $1 \leqslant k' \leqslant n'_i$ et $\lambda_{k',k}$ est la matrice d'un élément de $\mathrm{End}_{\mathbb{K}G}(S_i)$.

Invariants

La propriété que l'on s'apprête à prouver sera bientôt cruciale. Si W est un G-module, on a déjà introduit le sous-G-module des invariants :

$$W^G = \{w \in W,\ \forall g \in G,\ g\cdot w = w\}.$$

A.21. Proposition. *Soit W un espace vectoriel sur $\mathbb{K}$, corps de caractéristique nulle ou première à $|G|$. Soit $\rho : G \to \mathrm{GL}(W)$ une représentation. Alors, l'endomorphisme π défini par :*

$$\pi = \frac{1}{|G|}\sum_{g\in G} \rho(g)$$

est un morphisme de représentations et un projecteur dont l'image est W^G.

Démonstration. Soit $w \in W^G$, on a :

$$\pi(w) = \frac{1}{|G|}\sum_{g\in G} \rho(g)(w) = \frac{1}{|G|}\sum_{g\in G} w = w.$$

Et donc, $\pi|_{W^G} = \mathrm{Id}_{W^G}$. À présent, soit $w \in W$. On a, pour tout $h \in G$:

$$\pi\circ\rho(h)(w) = \frac{1}{|G|}\sum_{g\in G} \rho(gh)(w) = \frac{1}{|G|}\sum_{g'\in G} \rho(g')(w) = \pi(w)$$

et, de même :

$$\rho(h) \circ \pi(w) = \frac{1}{|G|} \sum_{g \in G} \rho(hg)(w) = \frac{1}{|G|} \sum_{g' \in G} \rho(g')(w) = \pi(w).$$

On en déduit l'inclusion : $\mathrm{im}(\pi) \subset W^G$. De cette inclusion et de la relation $\pi|_{W^G} = \mathrm{Id}_{W^G}$, on tire, comme en A.16, $\pi^2 = \pi$ et $\mathrm{im}\,\pi = W^G$. □

Il est naturel de se demander s'il existe un projecteur aussi explicite sur les composantes isotypiques d'une représentation. C'est un des apports de la théorie des caractères, voir le corollaire B.12. Nous allons maintenant présenter cette brillante et magistrale théorie.

Convention. On suppose désormais que le corps $\mathbb{K}$ est inclus dans $\mathbb{C}$.

B. Caractères

Le but de cette partie est d'introduire un outil particulièrement efficace pour étudier une représentation complexe d'un groupe fini G, son *caractère*. Il s'agit de calculer la trace des matrices de la représentation. Grâce à la semi-simplicité, nous allons voir que le caractère d'une représentation la caractérise, ce qui permet de résumer toute l'information[11] sous forme compacte dans la *table des caractères* de G.

Attention toutefois à ne pas surestimer ce bel outil. Si le caractère est capable de reconnaître une représentation, il ne la comprend qu'à isomorphisme près. Il serait illusoire de penser qu'une construction effective d'un choix de matrices représentatives soit chose facile. Voir le paragraphe 2.5 pour une telle construction sur un exemple.

B.1. Définition. Le *caractère* d'une représentation $\rho : G \to \mathrm{GL}(V)$ est la fonction :

$$\chi = \chi_V : G \to \mathbb{K}, \quad g \mapsto \mathrm{tr}\,\rho(g).$$

On dit que le caractère χ est *irréductible* si la représentation correspondante ρ est irréductible.

Commençons par exprimer les opérations sur les représentations en termes de caractères.

B.2. Lemme. *Soient V et V' deux représentations ; on note χ et χ' leurs caractères respectifs. Alors :*

(i) *si V et V' sont isomorphes, alors on a : $\chi = \chi'$;*

[11] La trace, c'est la classe !

(ii) *le caractère de la somme directe de V et V' est $\chi + \chi'$;*

(iii) *le caractère de la représentation duale de V est $\overline{\chi}$;*

(iv) *le caractère de $\mathrm{Hom}_{\mathbb{K}}(V, V')$ est $\overline{\chi}\chi'$.*

Démonstration. On va supposer pour simplifier que $\mathbb{K} = \mathbb{C}$. Pour le cas, général, où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, il suffira de travailler avec les complexifiés respectifs $V_{\mathbb{C}}$ et $V'_{\mathbb{C}}$ de V et V'.

Pour prouver l'assertion (i), on fixe un isomorphisme de représentations $\varphi : V \to V'$. Comme φ est un morphisme de représentations, pour tout g de G, la matrice de $\rho(g)$ dans une base (e_k) et celle de $\rho'(g)$ dans la base $(\varphi(e_k))$ (c'est bien une base, car φ est iso !) sont égales donc leurs traces sont égales. L'assertion (ii) est triviale dès que l'on sait que la trace d'une matrice diagonale par blocs est égale à la somme des traces des blocs diagonaux.

Pour prouver les assertions (iii) et (iv), nous allons prendre nos aises. Fixons un élément g de G et notons $N = |G|$. On a : $g^N = e$ dans G donc : $\rho(g)^N = \mathrm{Id}_V$. Par suite, $\rho(g)$ annule le polynôme scindé à racines simples $x^N - 1$ et $\rho(g)$ est diagonalisable. Fixons $(e_1, \ldots, e_d)$ une base de V formée de vecteurs propres de $\rho(g)$ et $\zeta_1, \ldots, \zeta_d$ les valeurs propres correspondantes. On choisit de même $(e'_1, \ldots, e'_{d'})$ et $(\zeta'_1, \ldots, \zeta'_{d'})$ pour V'. De la sorte :

$$\chi_\rho(g) = \sum_{j=1}^{d} \zeta_j, \quad \chi_{\rho'}(g) = \sum_{j=1}^{d} \zeta'_j.$$

Soit (e_j^*) la base duale de (e_j). On a, pour i et j entre 1 et d :

$$\rho^*(g)(e_j^*)(e_i) = e_j^*(\rho(g)^{-1}(e_i)) = \zeta_j^{-1}\delta_{i,j} \quad \text{(Kronecker)},$$

et donc : $\rho^*(g)(e_j^*) = \zeta_j^{-1} e_j^*$. Par suite, les valeurs propres sont les ζ_j^{-1} $(1 \leqslant j \leqslant d)$. Mais, les ζ_j sont des racines de l'unité, et leurs inverses sont donc leurs conjuguées. Ainsi :

$$\chi_{\rho^*}(g) = \sum_{j=1}^{d} \zeta_j^{-1} = \sum_{j=1}^{d} \overline{\zeta_j} = \overline{\chi_\rho(g)}.$$

Enfin, on choisit pour base de $\mathrm{Hom}_{\mathbb{K}}(V, V')$ la famille $(c_{jj'})$, où, si $1 \leqslant j \leqslant d$ et $1 \leqslant j' \leqslant d'$, on appelle $c_{jj'}$ l'application linéaire qui envoie e_j sur $e'_{j'}$ et tue e_k si $k \neq j$ (elle correspond aux matrices élémentaires). On a alors :

$$\rho'(g) \circ c_{jj'} \circ \rho(g)^{-1}(e_k) = \rho'(g) \circ c_{jj'}(\zeta_k^{-1} e_k) = \delta_{jk}\zeta_k^{-1}\rho'(g)(e'_{j'}) = \delta_{jk}\overline{\zeta_j}\zeta'_{j'} e'_{j'}.$$

En d'autres termes, $c_{jj'}$ est un vecteur propre pour l'action de g et sa valeur propre est $\overline{\zeta_j}\zeta'_{j'}$. Comme la famille $(c_{jj'})$ constitue une base de $\mathrm{Hom}_{\mathbb{K}}(V, V')$ (puisqu'elle correspond aux matrices élémentaires), on en déduit la valeur

du caractère de $\mathrm{Hom}_{\mathbb{K}}(V,V')$ en g :

$$\sum_{j=1}^{d}\sum_{j'=1}^{d'}\overline{\zeta_j}\zeta'_{j'} = \sum_{j=1}^{d}\overline{\zeta_j}\sum_{j'=1}^{d'}\zeta'_{j'} = \overline{\chi(g)}\chi'(g). \qquad \square$$

Fonction centrales et produit scalaire

B.3. Définition. On appelle *fonction centrale* une fonction $f : G \to \mathbb{C}$ qui est constante sur chaque classe de conjugaison :

$$\forall g,h \in G, \quad f(ghg^{-1}) = f(h).$$

B.4. Lemme

(i) *Les fonctions centrales forment une algèbre dont la dimension est le nombre de classes de conjugaison.*

(ii) *Les caractères sont des fonctions centrales.*

Démonstration. Pour la dimension, on remarque que les fonctions caractéristiques des classes de conjugaison forment une base de l'espace des fonctions centrales. La seconde assertion résulte de l'invariance de la trace par conjugaison. □

Voici l'outil qui rend la manipulation des caractères et la théorie des représentations complexes faciles.

B.5. Définition. On appelle *produit scalaire hermitien* de deux fonctions centrales χ et χ' le complexe :

$$\langle \chi,\chi' \rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\chi(g)}\,\chi'(g).$$

B.6. Remarque. Ce produit hermitien se prolonge naturellement en un produit sur l'espace $\mathbb{C}^G$ des fonctions complexes sur G tout entier. On note qu'il s'agit d'un produit invariant pour les action naturelles de G sur $\mathbb{C}^G$, par multiplication à droite, par conjugaison, etc.

L'essentiel de la théorie est résumé dans le fait que les caractères irréductibles constituent une base orthonormée de l'espace des fonctions[12] centrales (théorème C.7, ci-dessous).

[12]De la même manière que dans *Blanche-Neige*, Prof, Joyeux, Grincheux, Atchoum, Simplet, Dormeur et Timide constituent une base de caractères. Sauras-tu décomposer ton conjoint dans cette base ?

Morphismes invariants et caractères

B.7. Proposition. *Soient V et V' deux représentations complexes d'un groupe fini G, et soient χ et χ' leurs caractères respectifs. Alors :*

$$\langle \chi, \chi' \rangle = \dim \mathrm{Hom}_{\mathbb{C}}(V, V')^G = \dim \mathrm{Hom}_{\mathbb{C}G}(V, V').$$

Démonstration. La dernière égalité a été montrée dans la proposition A.6. Soit π le projecteur de la proposition A.21 pour $W = \mathrm{Hom}_{\mathbb{C}}(V, V')$. On a :

$$\begin{aligned} \dim \mathrm{Hom}_{\mathbb{C}}(V, V')^G &= \operatorname{rg} \pi \\ &= \operatorname{tr} \pi = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{Hom}_{\mathbb{C}}(V,V')}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi'(g) \\ &= \langle \chi, \chi' \rangle . \end{aligned}$$

□

Le corollaire suivant précise le lemme B.4, en exprimant que les caractères irréductibles forment une famille orthonormée dans l'espace des fonctions centrales.

Mise en garde. Notons que ces résultats sont valables sur $\mathbb{C}$. Les contre-exemples ne manquent pas sur $\mathbb{R}$, voir par exemple l'exercice F.9.

B.8. Corollaire. *Soient χ et χ' les caractères de deux représentations irréductibles V et V'. Alors :*

$$\langle \chi, \chi' \rangle = \begin{cases} 1 & \text{si } V \text{ et } V' \text{ sont isomorphes,} \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. On applique le lemme de Schur, proposition A.8, à la proposition précédente. □

Il est temps maintenant de voir que le mot « caractère » prend tout son sens, puisque le caractère d'une représentation complexe la caractérise à isomorphisme près ! Ce corollaire est donc une réciproque au lemme B.2 (i).

B.9. Corollaire. *Deux représentations sont isomorphes si et seulement si leurs caractères sont égaux.*

Plus précisément, si χ est le caractère de la représentation V et si les χ_i sont les caractères des irréductibles S_i pour tout i de $\mathrm{Irr}(G)$, alors

$$V \simeq \bigoplus_{i \in \mathrm{Irr}(G)} S_i^{m_i}, \quad \text{avec } m_i = \langle \chi_i, \chi \rangle.$$

Démonstration. Si deux représentations sont isomorphes, alors leurs caractères sont égaux, voir le lemme B.2 (i).

Montrons la réciproque. Par le théorème A.12 de Maschke, V se décompose, à isomorphisme près, en somme $V \simeq \bigoplus_{j\in \mathrm{Irr}(G)} S_j^{m_j}$. On a, par le corollaire B.8,

$$m_i = \langle \chi_i, \sum_j m_j \chi_j \rangle = \langle \chi_i, \chi_V \rangle.$$

Et donc, si la représentation W a même caractère que V, il vient

$$W \simeq \bigoplus_{i\in \mathrm{Irr}(G)} S_i^{\langle \chi_i, \chi_W\rangle} = \bigoplus_{i\in \mathrm{Irr}(G)} S_i^{\langle \chi_i, \chi_V\rangle} \simeq V. \qquad \square$$

En vertu de ce corollaire, on peut identifier les classes d'équivalence de représentations complexes irréductibles et leurs caractères, qui constituent l'ensemble $\mathrm{Irr}(G) = \mathrm{Irr}_{\mathbf{C}}(G)$.

B.10. Corollaire. *Pour tout i dans $\mathrm{Irr}(G)$, soit m_i la multiplicité de S_i dans la décomposition d'une représentation de caractère χ. Alors, on a :*

$$\sum_{i\in \mathrm{Irr}(G)} m_i^2 = \langle \chi, \chi \rangle.$$

En particulier, une représentation est irréductible si et seulement si son caractère est de norme 1.

Démonstration. On applique la formule $\chi = \sum_{i\in \mathrm{Irr}(G)} m_i \chi_i$ qui provient de l'additivité des caractères, et l'on développe $\langle \chi, \chi \rangle$. $\square$

B.11. Exercice. *Déduire, avec les notations du corollaire B.10, que si l'on a $\langle \chi, \chi \rangle = 2$ (resp. $\langle \chi, \chi \rangle = 3$), alors une représentation associée à χ se décompose en somme directe de deux (resp. trois) représentations irréductibles distinctes. Que peut-il se passer si $\langle \chi, \chi \rangle = 4$?*

Si $\langle \chi, \chi \rangle = 4$, la représentation se décompose soit en somme de quatre représentations irréductibles distinctes, soit une seule avec multiplicité 2.

B.12. Corollaire. *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation complexe de G. Alors, pour tout i dans $\mathrm{Irr}(G)$, l'endomorphisme π_i défini par*

$$\pi_i = \frac{\dim S_i}{|G|} \sum_g \overline{\chi_i(g)} \rho(g)$$

est un morphisme de représentations et un projecteur dont l'image est la composante isotypique de type i de V.

ELU PRODUIT EN FRANCE

Démonstration. L'endomorphisme π_i est bien un morphisme de représentations puisqu'il commute avec l'action de G :

$$\pi_i\rho(h) = \frac{\dim S_i}{|G|}\sum_{g\in G}\overline{\chi_i(g)}\rho(gh) = \frac{\dim S_i}{|G|}\sum_{k\in G}\overline{\chi_i(hkh^{-1})}\rho(hk)$$
$$= \frac{\dim S_i}{|G|}\rho(h)\sum_{k\in G}\overline{\chi_i(k)}\rho(k),$$

en posant $k = h^{-1}gh$ et en utilisant le fait qu'un caractère est invariant par conjugaison.

Soit V_j un sous-module irréductible de V isomorphe à S_j. Comme π_i est un morphisme de représentations, π_i stabilise V_j et comme V_j est irréductible, π_i agit comme une homothétie sur V_j. Le rapport de l'homothétie est

$$\lambda_{ij} = \frac{1}{\dim S_j}\operatorname{tr}\pi_i|_{V_j} = \frac{\dim S_i}{|G|\dim S_j}\sum_g \overline{\chi_i(g)}\chi_j(g) = \delta_{ij},$$

par le théorème d'orthogonalité. Le corollaire en résulte immédiatement.□

B.13. Remarque. La table des caractères de G, définie au §C.11, a des lignes indexées par les caractères irréductibles et des colonnes indexées par les classes de conjugaison. D'après la proposition, les lignes sont orthogonales. On verra que la table est carrée que ses colonnes sont aussi orthogonales en un sens convenable.

Nous allons terminer cette partie par deux constructions fort utiles de représentations (§B.14 et §B.20) et le calcul de leurs caractères.

B.14. Représentation par permutation

La construction qui vient est fondamentale : étant donnée une action de G, on fabrique une représentation. C'est l'incarnation la plus simple d'une idée profonde : une action intéressante donne lieu à des représentations intéressantes. Voici les applications que nous rencontrerons plus bas : au plan théorique, comprendre la représentation régulière permet, dans la partie C, de montrer que les caractères irréductibles forment une base de l'espace des fonctions centrales et de les compter ; en pratique, il est commode de disposer de « bonnes » actions pour calculer tous les caractères d'un groupe donné (pour un exemple frappant, voir l'exercice F.18 sur le groupe du cube).

Soit G un groupe fini agissant sur un ensemble fini X. La *représentation par permutation* associée à cette action est définie de la façon suivante. Soit $\mathbb{C}X$ l'espace vectoriel muni de sa base canonique $(e_x)_{x\in X}$ indexée par X. On

fait agir G de façon linéaire sur $\mathbb{C}X$ par :

$$\forall g \in G,\ \forall x \in X, \quad \rho_X(g)(e_x) = g \cdot e_x = e_{g\cdot x}.$$

La somme $s = \sum_{x\in X} e_x$ est invariante sous G, *i.e.* $\rho_X(g)(s) = s$ pour tout g de G. Elle engendre donc une droite qui est une sous-représentation isomorphe à la représentation triviale. On note V_X le quotient $\mathbb{C}X/\mathbb{C}s$ ou, ce qui revient au même à isomorphisme près, un supplémentaire de $\mathbb{C}s$ stable par le groupe G.

B.15. Proposition. *(Notations ci-dessus.)*

(i) *Le caractère χ de V_X est donné, pour g de G, par :* $\chi(g) = |X^g| - 1$.

(ii) *(Formule de Burnside à nouveau) On a :* $|X/G| = \sum_{g\in G} |X^g|/|G|$.

(iii) *Si G agit deux fois transitivement sur X, alors V_X est irréductible.*

ELU PRODUIT DE L'ANNÉE

Démonstration. (i) Si l'on écrit la matrice de $\rho_X(g)$ ($g \in G$) dans la base $(e_x)_{x\in X}$, le coefficient diagonal d'indice x vaut 1 si g fixe x et 0 sinon. Par suite, la trace d'un élément de G agissant dans $\mathbb{C}X$ est le nombre de points fixes pour l'action de G sur X. Le résultat en découle par additivité des caractères.

(ii) Considérons l'espace $(\mathbb{C}X)^G$ des invariants de l'espace $\mathbb{C}X$. Un vecteur $\sum_{x\in X} \lambda_x e_x$ est invariant par G si et seulement si pour tout g de G et tout x de X, on a : $\lambda_x = \lambda_{g\cdot x}$. Il est donc nécessaire et suffisant que l'application $\lambda : X \to \mathbb{C}$, $x \mapsto \lambda_x$ soit constante sur les orbites, d'où : $\dim(\mathbb{C}X)^G = |X/G|$.

À présent, soit e l'endomorphisme de $\mathbb{C}X$ défini par : $e = \dfrac{1}{|G|} \sum_{g\in G} \rho_X(g)$. On a vu que e est un projecteur sur $(\mathbb{C}X)^G$. Il vient :

$$|X/G| = \dim(\mathbb{C}X)^G = \operatorname{rg}(e) = \operatorname{tr} e = \frac{1}{|G|} \sum_{g\in G} |X^g|.$$

Pour la dernière égalité, on note que, comme $\rho_X(g)(e_x) = e_{g\cdot x}$, la trace de $\rho_X(g)$, que l'on calcule dans la base $(e_x)_{x\in X}$, est égale à $|X^g|$.

(iii) Notons χ le caractère de V_X. On a :

$$\langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g\in G} (|X^g| - 1)^2 = \frac{1}{|G|} \sum_{g\in G} |X^g|^2 - 2\frac{1}{|G|} \sum_{g\in G} |X^g| + 1.$$

Comme l'action de G est transitive, d'après la formule de Burnside, on a :

$$\frac{1}{|G|} \sum_{g} |X^G| = |X/G| = 1.$$

Pour la première, on fait agir G sur $X \times X$ diagonalement, c'est-à-dire que $g \cdot (x, y) = (g \cdot x, g \cdot y)$ pour g de G et x, y de X. L'hypothèse de double-

transitivité se traduit par le fait que G a deux orbites dans $X \times X$: la diagonale $\Delta = \{(x,x),\ x \in X\}$ et son complémentaire.

On remarque que l'on a : $(X \times X)^g = X^g \times X^g$ pour tout g. Appliquons la formule de Burnside à $X \times X$:

$$\frac{1}{|G|} \sum_{g \in G} |X^g|^2 = \frac{1}{|G|} \sum_{g \in G} |(X \times X)^g| = |(X \times X)/G| = 2,$$

d'où l'on tire : $\langle \chi, \chi \rangle = 2 - 2 + 1 = 1$. Ainsi, V_X est irréductible, par le corollaire B.10. □

B.16. Remarque. Plus généralement, on montre par le même calcul que si G agit transitivement sur X, alors la norme $\langle \chi, \chi \rangle$ du caractère de V_X est égal au nombre d'orbites de G pour l'action diagonale sur $(X \times X) \setminus \Delta$. Pour en donner un exemple frappant et instructif, on voit dans l'exercice F.49 que pour l'action du groupe des isométries positives d'un cube sur les faces du cube, on obtient : $\langle \chi, \chi \rangle = 2$, ce qui correspond à l'action sur les paires distinctes de faces, qui possède deux orbites constituées respectivement des faces adjacentes et des faces opposées du cube.

B.17. Exercice (Probabilités et représentations)

1. *Quel est en moyenne le nombre d'éléments fixés par une permutation ?* Eh bien, $n!^{-1} \sum_{\sigma \in \mathfrak{S}_n} |X^\sigma| = 1$, bien sûr, par la formule de Burnside... puisque l'action de $\mathfrak{S}_n$ sur $X = \{1, \dots, n\}$ est transitive.
2. *Quelle est la variance du nombre d'éléments fixés par une permutation ?* Facile : $n!^{-1} \sum_{\sigma \in \mathfrak{S}_n} |X^\sigma|^2 - \left(n!^{-1} \sum_{\sigma \in \mathfrak{S}_n} |X^\sigma|\right)^2 = 2 - 1^2 = 1$, encore par la formule de Burnside... puisque l'action de $\mathfrak{S}_n$ sur X est doublement transitive.
3. *Généraliser ce résultat pour toute action d'un groupe fini G sur un ensemble fini X.*

   La moyenne m est égale au nombre d'orbites de G sur X et la variance vaut $v = k - m^2$, où k désigne le nombre d'orbites de G pour l'action diagonale sur $X \times X$. En termes de représentations, si $\mathbb{C}X$ est la représentation par permutation, qui se décompose en $W \oplus W^\perp$, où W désigne la composante isotypique G-invariante, alors $m = \sqrt{\langle \chi_W, \chi_W \rangle_G}$ et $v = \langle \chi_{W^\perp}, \chi_{W^\perp} \rangle_G$.

Pour conclure sur les représentations par permutation, signalons que l'idée sous-jacente se décline dans la théorie des groupes de Lie. Lorsqu'un groupe de Lie G agit de façon géométrique sur une variété X, il préserve les invariants géométriques : espaces de fonctions, distributions, formes différentielles, espaces de cohomologie... L'action des groupes algébriques comme

les groupes $\mathrm{GL}_n(\mathbb{K})$ sur leur « variété des drapeaux » est le point de départ de la classification des représentations de la forme $G \to \mathrm{GL}_N(\mathbb{K})$ dont les coefficients matriciels sont des polynômes en ceux de G.

B.18. Caractère des formes bilinéaires symétriques

Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G. L'exemple (e) du §A.2 fait de l'espace $\mathrm{Bil}_{\mathrm{s}}(V)$ des formes bilinéaires symétriques[13] sur V une représentation de G. Normal ! La congruence définit une action linéaire de $\mathrm{GL}(V)$ sur l'espace des formes, c'est-à-dire un morphisme $\Phi : \mathrm{GL}(V) \to \mathrm{GL}\big(\mathrm{Bil}_{\mathrm{s}}(V)\big)$, que l'on peut composer avec ρ. Rappelons que si β est une forme bilinéaire (symétrique ou alternée) sur V et si g est un élément de g, l'action de g sur β est définie par :

$$\forall v, v' \in V, \quad g \cdot \beta(v, v') = \beta\big(\rho(g^{-1})v, \rho(g)^{-1}v'\big).$$

On va calculer le caractère de cette représentation en fonction de celui de G.

B.19. Lemme. *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G de caractère χ.*

(i) *Le caractère de $\mathrm{Bil}_{\mathrm{s}}(V)$ est : $\Psi : g \mapsto \dfrac{\chi(g^{-1})^2 + \chi(g^{-2})}{2}$.*

(ii) *Soit $\mathbf{e}$ une base de V. Soit β une forme bilinéaire symétrique sur V et soit B sa matrice dans $\mathbf{e}$. Soit g un élément de G et soit $\rho_0(g)$ la matrice de $\rho(g)$ dans $\mathbf{e}$. Alors, la matrice de $g \cdot \beta$ dans $\mathbf{e}$ est ${}^t\rho_0(g)^{-1} B \rho_0(g)^{-1}$.*

Démonstration. (i) Soit g un élément de G. Pour calculer la trace de l'automorphisme $\Phi \circ \rho(g)$ associé à g, on peut choisir n'importe quelle base de l'espace de $\mathrm{Bil}_{\mathrm{s}}(V)$. On en fabrique une qui est bien adaptée à g. Comme g est d'ordre fini, $\Phi \circ \rho(g)$ est diagonalisable. Soit $\mathbf{e} = (e_1, \dots, e_n)$ une base de V formés de vecteurs propres et soient $\lambda_1, \dots, \lambda_n$ les valeurs propres correspondantes. L'application « matrice dans la base $\mathbf{e}$ » est un isomorphisme linéaire de $\mathrm{Bil}_{\mathrm{s}}(V)$ sur l'espace $\mathscr{S}_n(\mathbb{C})$ des matrices symétriques, dont une base est constituée des matrices $S^{i,i} = E^{i,i}$ $(1 \leqslant i \leqslant n)$ et des $S^{i,j} = E_{ij} + E_{ji}$ $(1 \leqslant i < j \leqslant n)$, où les E_{ij} sont les matrices élémentaires. Leur correspondent les formes $\beta^{i,i}$ et $\beta^{i,j}$, qui sont caractérisées par :

$$\beta^{i,j}(e_k, e_\ell) = \begin{cases} 1 & \text{si } \{i,j\} = \{k,\ell\} \\ 0 & \text{sinon} \end{cases} \qquad \big(i, j, k, \ell \in \{1, \dots, n\},\ i \leqslant j\big).$$

[13] Dans ce paragraphe, nous nous restreignons aux formes symétriques parce qu'elles sont plus familières.

On en tire immédiatement : $g\cdot\beta^{i,j}=\lambda_i^{-1}\lambda_j^{-1}$ lorsque $1\leqslant i\leqslant j\leqslant n$. Ainsi, la trace de l'action de g est :

$$\sum_{1\leqslant i\leqslant j\leqslant n}\frac{1}{\lambda_i\lambda_j}=\sum_{i=1}^{n}\frac{1}{\lambda_i^2}+\sum_{i<j}\frac{1}{\lambda_i\lambda_j}=\frac{1}{2}\Big(\sum_{i=1}^{n}\frac{1}{\lambda_i}\Big)^2+\frac{1}{2}\sum_{i=1}^{n}\frac{1}{\lambda_i^2}$$
$$=\frac{\chi(g^{-1})^2+\chi(g^{-2})}{2}.$$

(ii) C'est simplement l'expression matricielle de la congruence. Si v et v' sont deux vecteurs de V ayant pour coordonnées X et X' dans $\mathbf{e}$, on a par définition : $\beta(v,v')={}^tXBX'$. Faisons agir un élément g de G :

$$\begin{aligned}g\cdot\beta(v,v')&=\beta\big(\rho(g^{-1})v,\rho(g^{-1})v'\big)\\&={}^t\big(\rho_0(g)^{-1}X\big)B\big(\rho_0(g)^{-1}X'\big)\\&={}^tX\,{}^t\rho_0(g)^{-1}B\rho_0(g)^{-1}X',\end{aligned}$$

et l'on peut conclure, car v et v' sont quelconques. □

B.20. Carré symétrique et carré alterné d'une représentation

Voici une construction de deux représentations associées à une représentation donnée. Elle nous sera utile pour calculer les caractères de groupes concrets, mais aussi pour des questions théoriques dans la partie E.

On peut simplifier la formule du lemme B.19 (ii). On part d'une représentation matricielle $\rho_0 : G\to\mathrm{GL}_n(\mathbb{C})$. On fait agir G sur l'espace $\mathscr{M}_n(\mathbb{C})$ de la façon suivante :

$$\forall g\in G,\ \forall M\in\mathscr{M}_n(\mathbb{C}),\quad g\cdot M=\rho_0(g)M\,{}^t\rho_0(g).$$

L'espace des matrices est la somme directe des sous-espaces des matrices symétriques et des matrices alternées : $\mathscr{M}_n(\mathbb{C})=\mathscr{S}_n(\mathbb{C})\oplus\mathscr{A}_n(\mathbb{C})$. Depuis [H2G2, chapitre V], on sait que l'on définit bien ainsi une action linéaire ; de plus, $\mathscr{S}_n(\mathbb{C})$ et $\mathscr{A}_n(\mathbb{C})$ sont des sous-G-modules de $\mathscr{M}_n(\mathbb{C})$. On note les deux représentations respectives associées $\mathrm{S}^2\rho_0 : G\to\mathrm{GL}\big(\mathscr{S}_n(\mathbb{C})\big)$ et $\bigwedge^2\rho_0 : G\to\mathrm{GL}\big(\mathscr{A}_n(\mathbb{C})\big)$.

Remarque. Il sera utile dans la suite de voir que ces deux représentations ainsi définies ne dépendent, à isomorphisme près, que de la classe d'isomorphisme de ρ_0. En effet, si P est une matrice inversible fixée et si l'on remplace ρ_0 par $\rho_0' : G\to P\rho_0(g)P^{-1}$, l'isomorphisme linéaire $A\mapsto PA\,{}^tP$

est un isomorphisme pour les G-modules définis par ρ_0 et ρ'_0 :

$$\begin{aligned} P\rho_0(g)A\,{}^t\rho_0(g)\,{}^tP &= P\rho_0(g)P^{-1}\,PA\,{}^tP\,{}^tP^{-1}\,{}^t\rho_0(g)\,{}^tP \\ &= \rho'_0(g)PA\,{}^tP\,{}^t\rho'_0(g). \end{aligned}$$

Cela permet de définir $\mathrm{S}^2\rho$ (resp. $\bigwedge^2\rho$) pour une représentation $\rho : G \to \mathrm{GL}(V)$ quelconque, au moins à isomorphisme près. En effet, ρ étant donnée, on choisit une base $\mathbf{e} = (e_1, \ldots, e_n)$ de V, ce qui donne une représentation matricielle $\rho_0 : G \to \mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(\mathbb{C})$. On vient de vérifier que la représentation matricielle $\mathrm{S}^2\rho_0$ (resp. $\bigwedge^2\rho_0$) ne dépend pas, à isomorphisme près, du choix de $\mathbf{e}$. C'est cette représentation, que l'on note $\mathrm{S}^2\rho$ (resp. $\bigwedge^2\rho$) et que l'on appelle *carré symétrique* (resp. *carré alterné*) de la représentation ρ.

On va reconnaître ces représentations. Bien sûr, cela ressemble aux formes bilinéaires du lemme B.19. Mais comme on a remplacé la matrice ${}^t\rho_0(g)^{-1}$ par $\rho_0(g)$ « pour simplifier », cela revient[14] à remplacer $\rho_0(g)$ par ${}^t\rho_0(g)^{-1}$, c'est-à-dire V par son dual V^*.

Dans la proposition suivante, on voit donc intervenir les formes bilinéaires sur le dual... Si l'on essaie de penser un tel objet comme une application linéaire du dual vers le bidual, c'est vertigineux. Pas de panique ! C'est aussi tout à fait inutile ! Il faut ici concevoir le dual V^* comme un espace vectoriel de même dimension que V sur lequel G agit différemment — les nouvelles matrices sont les transposées des inverses de celles qui définissent l'action sur V.

B.21. Proposition. *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation et soit χ son caractère.*

(i) *Pour tout g de G, on a :*

$$\mathrm{tr}\,\mathrm{S}^2\rho(g) = \frac{\chi(g)^2 + \chi(g^2)}{2}, \quad \mathrm{tr}\bigwedge{}^2\rho(g) = \frac{\chi(g)^2 - \chi(g^2)}{2}.$$

(ii) *On a des isomorphismes de représentations :*

$$\mathrm{S}^2\rho \oplus \bigwedge{}^2\rho \simeq \mathscr{S}_n(\mathbb{C}) \oplus \mathscr{A}_n(\mathbb{C}) \simeq \mathrm{Bil}(V^*).$$

(iii) *La représentation $\mathrm{S}^2\rho$ (resp. $\bigwedge^2\rho$) est isomorphe aux formes bilinéaires symétriques (resp. alternées) sur V^* (§A.2 (e)).*

(iv) *Si ρ est irréductible, la somme des multiplicités de la représentation triviale dans $\mathrm{S}^2\rho$ et dans $\bigwedge^2\rho$ est au plus* 1.

[14] Eh ! C'est que l'application $X \mapsto {}^tX^{-1}$ est une involution du groupe linéaire $\mathrm{GL}_n(\mathbb{C})$.

Démonstration. (i) On introduit les matrices élémentaires E_{ij}, pour i et j compris entre 1 et n. Si $1 \leqslant i \leqslant j \leqslant n$, on pose $S^{i,j} = E_{ij} + E_{ji}$. Si $1 \leqslant i < j \leqslant n$, on pose : $A^{i,j} = E_{ij} - E_{ji}$. On retrouve les bases habituelles de $\mathscr{S}_n(\mathbb{C})$ et de $\mathscr{A}_n(\mathbb{C})$.

Soit g dans G. Comme $\rho(g)$ est d'ordre fini, c'est une matrice diagonalisable. Quitte à conjuguer ρ par une matrice inversible P bien choisie, ce qui ne change pas la classe d'isomorphisme de ρ et en particulier pas son caractère, on peut supposer que $\rho(g)$ est diagonale (voir la remarque dans le §B.20). Soient $\lambda_1, \ldots, \lambda_n$ ses valeurs propres. Connaissant le lien entre produit par une matrice et opérations élémentaires sur les rangées, pour une matrice $A = (a_{ij})$, on trouve de tête que le coefficient d'indice (i,j) de $\rho(g)A\,{}^t\rho(g)$ est $\lambda_i\lambda_j a_{ij}$. Par conséquent, il vient que $S^{i,j}$ (resp. $A^{i,j}$) est un vecteur propre de $\mathrm{S}^2\rho(g)$ (resp. de $\bigwedge^2\rho(g)$) pour la valeur propre $\lambda_i\lambda_j$ dès que $1 \leqslant i \leqslant j \leqslant n$ (resp. $1 \leqslant i < j \leqslant n$).

La trace de $\mathrm{S}^2\rho(g)$ est donc :

$$\sum_{1\leqslant i\leqslant j\leqslant n} \lambda_i\lambda_j = \sum_{i=1}^{n} \lambda_i^2 + \sum_{1\leqslant i<j\leqslant n} \lambda_i\lambda_j = \frac{1}{2}\Big(\sum_{i=1}^{n}\lambda_i\Big)^2 + \frac{1}{2}\sum_{i=1}^{n}\lambda_i^2 = \frac{\chi(g)^2+\chi(g^2)}{2},$$

alors que celle de $\bigwedge^2\rho(g)$ est :

$$\sum_{1\leqslant i<j\leqslant n} \lambda_i\lambda_j = \frac{1}{2}\Big(\sum_{i=1}^{n}\lambda_i\Big)^2 - \frac{1}{2}\sum_{i=1}^{n}\lambda_i^2 = \frac{\chi(g)^2-\chi(g^2)}{2}.$$

(ii)–(iii) Soit $\mathbf{e} = (e_i)_{1\leqslant i\leqslant n}$ une base de V et soit $\mathbf{e}^*$ sa base duale dans V^*. Pour définir $\mathrm{S}^2\rho$ et $\bigwedge^2\rho$, on a fait agir G sur les matrices par une sorte de congruence, ce qui évoque les formes bilinéaires. Il y a ici une difficulté : au §A.2, on a fait de l'espace $\mathrm{Bil}(V)$ un G-module, mais au niveau matriciel, l'action d'un élément g sur la matrice B d'une forme est (exercice A.4) : ${}^t\rho_0(g)^{-1}B\rho_0(g)^{-1}$ — ce n'est pas l'action que nous souhaitons. C'est pourquoi il faut faire intervenir le dual.

L'application « matrice dans $\mathbf{e}^*$ » est une isomorphisme $\mathrm{mat}_{\mathbf{e}^*}$ linéaire de l'espace $\mathrm{Bil}(V^*)$ des formes bilinéaires sur V^* sur $\mathscr{M}_n(\mathbb{C})$. Il envoie l'espace des formes symétriques (resp. alternées) sur $\mathscr{S}_n(\mathbb{C})$ (resp. $\mathscr{A}_n(\mathbb{C})$). Mais, tous ces espaces sont des G-modules : vérifions que $\mathrm{mat}_{\mathbf{e}^*}$ est un morphisme de représentations.

Soit β une forme bilinéaire sur V^* et soit $B = \mathrm{mat}_{\mathbf{e}^*}(\beta)$. Soit g un élément de G. D'après l'exercice A.4 appliqué à V^*, la matrice de $g\cdot\beta$ est donnée, en fonction de la matrice $\check{\rho}_0(g) = {}^t\rho_0(g)^{-1}$ de l'action de g dans V^*, par :

$$\mathrm{mat}_{\mathbf{e}^*}(\beta) = {}^t\check{\rho}_0(g^{-1})B\check{\rho}_0(g^{-1}) = \rho_0(g)B\,{}^t\rho_0(g) = g\cdot\mathrm{mat}_{\mathbf{e}^*}(\beta).$$

(iv) Si la représentation V est irréductible, sa duale V^* l'est aussi puisque l'on a : $\langle\overline{\chi},\overline{\chi}\rangle = \langle\chi,\chi\rangle = 1$. Par le lemme de Schur, il existe au plus un

morphisme de représentations (à scalaire près) de V^* sur V. On conclut avec l'assertion (iii). □

B.22. Remarque. Avec les notations de la preuve précédente, on vérifie par un calcul facile que lorsque la matrice $\rho_0(g)$ de $\rho(g)$ dans une base quelconque est $(g_{ij})_{1\leqslant i,j\leqslant n}$, on a :

$$g\cdot S^{i_0,j_0} = \sum_{1\leqslant i\leqslant j\leqslant n} (g_{ii_0}g_{jj_0} + g_{ij_0}g_{ji_0})S^{i,j} \qquad (1\leqslant i_0\leqslant j_0\leqslant n),$$

$$g\cdot A^{i_0,j_0} = \sum_{1\leqslant i<j\leqslant n} (g_{ii_0}g_{jj_0} - g_{ij_0}g_{ji_0})A^{i,j} \qquad (1\leqslant i_0< j_0\leqslant n).$$

Cela signifie que le coefficient d'indice $\big((i,j),(i_0,j_0)\big)$ de la matrice $\rho_0(g)$ est $g_{ii_0}g_{jj_0} \pm g_{ij_0}g_{ji_0}$. En particulier, si toutes les matrices $\rho_0(g)$ sont à coefficients réels, il en est de même des matrices $\mathsf{S}^2\rho_0(g)$ et $\bigwedge^2\rho_0(g)$.

B.23. Remarque. L'assertion (ii) du lemme montre que l'on a triché : on aurait dû définir $\mathsf{S}^2\rho$ et $\bigwedge^2\rho$ en termes de formes bilinéaires pour avoir des représentations naturelles, plutôt que passer par les matrices. Mais la méthode choisie a l'avantage d'être plus terre à terre.

Les carrés symétriques et alternés, comme l'espace des morphismes et le dual, sont des cas particuliers de constructions très générales dites *tensorielles*, dont on verra la pierre angulaire au §XI-A.1. L'art consistant à comprendre de telles représentations est appelé le *pléthysme*[15].

C. « La somme des carrés »

Le résultat principal de cette partie, point culminant de la théorie des représentations complexes, exprime que les caractères irréductibles forment une base orthonormée de l'espace des fonctions centrales. Il en résulte presque immédiatement qu'il y a autant de fonctions centrales que de classes de conjugaison — autrement dit, la table des caractères est carrée.

La partie commence par un ingrédient essentiel pour démontrer le théorème, la représentation régulière et sa décomposition en irréductibles. Puis, on déroule la théorie et l'on termine par une mise en perspective de ces résultats dans le contexte de l'analyse harmonique.

[15] Il s'agit de la francisation de l'anglais *plethysm*, introduit quelque peu mystérieusement par Littlewood à partir du grec πληθυσμός signifie *population*. Le mot français est presque un apax. Robert Bonnaud, dans *Le système de l'histoire* (Fayard, 1989), définit cette doctrine comme « le choix de la "peuplade", de la masse humaine, de sa préservation, de son accroissement ».

C.1. Représentation régulière

Nous l'avons déjà vu : la *représentation régulière* ρ_{reg} de G est la représentation par permutation associée à l'action de G sur lui-même par multiplication à gauche. L'espace ambiant est le $\mathbb{C}$-espace $\mathbb{C}G$, qui admet pour base $(\delta_g)_{g\in G}$. L'action d'un élément g de G est définie par :

$$\forall h \in G, \quad \rho_{\text{reg}}(g)(\delta_h) = \delta_{gh}.$$

C.2. Remarque. On peut interpréter autrement cette représentation. L'espace ambiant peut être identifié à l'espace $\mathbb{C}^G$ des fonctions de G dans $\mathbb{C}$, muni de sa structure de $\mathbb{C}$-espace naturel et muni de l'action linéaire de G par

$$g \cdot f = f(?g) \ (g \in G,\ f \in \mathbb{C}^G).$$

On a alors un isomorphisme ι de G-représentations entre $\mathbb{C}G$ et $\mathbb{C}^G$ qui à δ_h ($h \in G$) associe l'application définie par $\iota(\delta_h)(g) = \delta_{h^{-1},g}$ (le deuxième δ est le symbole de Kronecker). On généralisera cette construction avec les représentations induites dans l'exercice XI-C.4.

Si g est un élément non trivial de G, tous les coefficients diagonaux de la matrice de $\rho_{\text{reg}}(g)$ dans la base $(\delta_h)_{h\in G}$ sont nuls[16]. On en déduit le caractère de la représentation régulière.

C.3. Lemme. *Soit χ_{reg} le caractère de la représentation régulière. On a :*

$$\forall g \in G, \quad \chi_{\text{reg}}(g) = \begin{cases} |G| & \text{si } g = e, \\ 0 & \text{sinon.} \end{cases}$$

La simplicité de l'expression de χ_{reg} permet de décomposer facilement la représentation régulière. Soit χ un caractère irréductible et soit V_χ une représentation correspondante. On a, par C.3 :

$$\langle \chi, \chi_{\text{reg}} \rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\chi(g)}\chi_{\text{reg}}(g) = \overline{\chi(e)} = \dim V_\chi.$$

En particulier, toute représentation irréductible apparaît dans la représentation régulière, si bien que le nombre de représentations irréductibles à isomorphisme près est fini. Écrivons dans ce cas la décomposition de la proposition A.18.

[16] Cela provient entre autres du fait que tout élément d'un groupe est « régulier ». De là à croire que c'est l'origine de l'appellation, il n'y a qu'un pas. En tout cas, une chose est sûre, la régulière est fidèle !

C.4. Proposition. *On a un isomorphisme de G-modules :*

$$\mathbb{C}G \simeq \bigoplus_{\chi \in \mathrm{Irr}(G)} (V_\chi)^{\chi(e)}.$$

On tire quelques conséquences de l'égalité $\chi(e) = \dim V_\chi$.

C.5. Corollaire. *On a :*

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(e) \dim V_\chi = \sum_{\chi \in \mathrm{Irr}(G)} \chi(e)^2.$$

Et, si g est un élément de G différent du neutre e, on a :

$$0 = \chi_{\mathrm{reg}}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(g) \dim V_\chi = \sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\chi(e).$$

C.6. Remarque. Ironie : la représentation régulière contient toutes les représentations irréductibles, donc toutes les informations que l'on aimerait connaître. Pourtant le caractère de la régulière est trivial à calculer ! Cela peut rappeler une autre situation également issue de l'action d'un groupe par multiplication à gauche sur lui-même : tout groupe fini est sous-groupe du gentil groupe des permutations. Cet infiniment difficile incrusté dans l'infiniment simple finit par engendrer une certaine frustration, non ?

Le théorème suivant est essentiel pour espérer calculer les caractères irréductibles d'un groupe fini. Rappelons que d'après le lemme de Schur, reformulé dans le lemme B.4 et le corollaire B.8 la famille formée des caractères irréductibles est une famille orthonormée de l'espace des fonctions centrales sur G, muni du produit hermitien $\langle \cdot, \cdot \rangle$. Cette famille est donc libre. En fait, c'est même une base.

C.7. Théorème. *L'ensemble des caractères irréductibles de G est une base orthonormée de l'espace des fonctions centrales.*

Donnons tout de suite un corollaire important à ce théorème.

C.8. Corollaire. *Le nombre de représentations complexes irréductibles de G à isomorphisme près est égal au nombre de classes de conjugaison.*

Démonstration (du corollaire). La dimension de l'espace des fonctions centrales est le nombre de classes de conjugaison de G, par le lemme B.4. □

La preuve qui suit est tirée de [76].

C.9. Lemme. *Soit f une fonction centrale sur G et soit $\rho : G \to \mathrm{GL}(V)$ une représentation. Soit*

$$\rho_f = \frac{1}{|G|} \sum_{g \in G} f(g)\rho(g) \in \mathrm{End}_{\mathbb{C}}(V).$$

Alors :

(i) *ρ_f est un morphisme de représentations,* i.e. $\rho_f \in \mathrm{End}_{\mathbb{C}G}(V)$;

(ii) *si V est irréductible de caractère χ, alors ρ_f est une homothétie et son rapport est $\langle \overline{\chi}, f \rangle / \chi(e)$.*

Démonstration (du lemme). Montrons que ρ_f commute avec tous les $\rho(h)$ ($h \in G$). En effet (on fait le changement d'indice $g = hkh^{-1}$, qui donne $gh = hk$) :

$$\begin{aligned} \rho_f \rho(h) &= \frac{1}{|G|} \sum_{g \in G} f(g)\rho(gh) = \frac{1}{|G|} \sum_{k \in G} f(hkh^{-1})\rho(hk) \\ &= \frac{1}{|G|} \sum_{k \in G} f(k)\rho(h)\rho(k) = \rho(h)\rho_f. \end{aligned}$$

Si l'on suppose que V est irréductible, alors, par le lemme de Schur, ρ_f est une homothétie. Son rapport λ est lié à sa trace :

$$\lambda = \frac{1}{\dim(V)} \operatorname{tr} \rho_f = \frac{1}{\chi(e)} \frac{1}{|G|} \sum_{g \in G} f(g)\chi(g) = \frac{\langle \overline{\chi}, f \rangle}{\chi(e)}. \qquad \square$$

Démonstration (du théorème). On a déjà vu que l'ensemble des caractères irréductibles est une famille orthonormée de l'espace des fonctions centrales. Pour montrer qu'elle est génératrice, il suffit de montrer que toute fonction centrale $f : G \to \mathbb{C}$ qui est orthogonale à tous les caractères irréductibles est nulle. Soit f une telle fonction. Pour toute représentation ρ, on définit ρ_f comme dans le lemme. Si ρ est irréductible, alors, par le lemme, ρ_f est nulle car le produit scalaire est nul (rappelons que le conjugué $\overline{\chi}$ d'un caractère irréductible χ est encore un caractère irréductible par dualité des représentations). Si ρ est une somme directe d'irréductibles, alors, d'après ce qui précède, ρ_f est nulle sur chaque composante irréductible de V, donc ρ_f est nulle. Mais par le théorème de Mashke, toute représentation est somme directe d'irréductibles, donc ρ_f est toujours nulle.

Prenons pour ρ la représentation régulière et calculons $\rho_f(\delta_e)$:

$$0 = \rho_f(\delta_e) = \frac{1}{|G|} \sum_{g \in G} f(g)\rho(g)(\delta_e) = \frac{1}{|G|} \sum_{g \in G} f(g)\delta_g.$$

Par indépendance linéaire de $(\delta_g)_{g \in G}$, on a : $f(g) = 0$ pour tout g, ce qui termine la preuve. $\square$

C.10. Exercice. *On associe, à tout élément σ du groupe symétrique $\mathfrak{S}_n$, la* partition $p(\sigma)$ *de n donnée par les longueurs des cycles de la décomposition en cycles disjoints de σ. Par exemple, si $\sigma = (264)(17) \in \mathfrak{S}_7$, on obtient la partition $p(\sigma) = (3 \geqslant 2 \geqslant 1 \geqslant 1)$ de 7.*

1. *Montrer par la formule de conjugaison que deux permutations sont conjuguées si et seulement si elles ont même partition associée.*
2. *En déduire que le nombre de représentations irréductibles de $\mathfrak{S}_n$ est égal au nombre $p(n)$ de partitions de n.*

Pub ! La série génératrice des $p(n)$ est dans [H2G2, §III-2.6].

C.11. La table des caractères vue comme matrice carrée

Il est commode de résumer l'information sur les représentations de G dans un tableau appelé *table des caractères.* Ses lignes sont indexées par les caractères irréductibles, ses colonnes par les classes de conjugaison. Le corollaire C.8 montre que *cette table est carrée.* En ordonnant les classes de conjugaison $(C_j)_{1\leqslant j\leqslant h}$ de G et ses caractères irréductibles $(\chi_i)_{1\leqslant i\leqslant h}$, on forme la matrice $U = (u_{ij})_{1\leqslant i,j\leqslant h}$ dont la composante u_{ij} est la valeur de χ_i sur C_j.

On peut alors reformuler et prolonger le corollaire B.8 sur l'orthogonalité des caractères.

C.12. Corollaire. *Soit $U = (u_{ij})_{1\leqslant i,j\leqslant h}$ la table de caractères de G, et soit D la matrice diagonale $D = \operatorname{diag}\big(|C_j|\big)_{1\leqslant j\leqslant h}$. Alors, on a :*

(i) $UDU^* = |G|\mathrm{I}_h$;

(ii) $U^*U = |G|D^{-1}$;

(iii) *étant donnés deux éléments g et g' de G,*

$$\sum_i \overline{\chi_i(g)}\chi_i(g') = \begin{cases} \dfrac{|G|}{|C_j|} & \text{si } g, g' \in C_j, \\ 0 & \text{si } g \text{ et } g' \text{ non conjugués.} \end{cases}$$

Démonstration. L'assertion (i) est une reformulation du corollaire B.8. L'assertion (ii) s'en déduit puisque, par passage à l'inverse $(U^*)^{-1}D^{-1}U^{-1} = |G|^{-1}\mathrm{I}_h$, et enfin $|G|D^{-1} = U^*U$. L'assertion (iii) est une reformulation de (ii). □

C.13. Exemples. On trouve de nombreux exemples de constructions des tables de caractères pour des groupes de petits cardinaux dans les chapitres et XI et leurs exercices.

C.14. Exercice. *Comment compléter la table des caractères d'un groupe lorsqu'il ne manque qu'une représentation irréductible ?*

Deux méthodes faciles à mettre en œuvre :

- on commence par trouver la dimension de la représentation par la formule de la somme des carrés, puis l'équation (iii) du corollaire C.12 fournit la dernière ligne de U via de petites équations à une inconnue !
- on utilise la représentation régulière, voir le corollaire C.5.

C.15. Un peu de philosophie : analyse harmonique

Au bilan, on a deux bases naturelles pour l'algèbre des fonctions centrales : les fonctions indicatrices des classes de conjugaison et les caractères. Le passage d'une base à l'autre est hautement non trivial, en particulier parce que les ensembles d'indices sont très différents. Néanmoins, le théorème C.7 exprime que toute fonction centrale $f : G \to \mathbb{C}$ s'exprime dans la base orthonormée des caractères de la façon suivante :

$$(F) \qquad f = \sum_{\chi \in \mathrm{Irr}(G)} \hat{f}(\chi)\chi, \quad \text{où } \hat{f}(\chi) = \langle \chi, f \rangle \ \big(\chi \in \mathrm{Irr}(G)\big).$$

Observons le cas spécial du groupe $\mathbb{Z}/n\mathbb{Z}$: comme il est abélien, toute fonction est centrale et il y a n caractères. On compare donc les bases δ_k ($k \in \mathbb{Z}/n\mathbb{Z}$, le δ de Kronecker) et $\chi_\ell : k \mapsto \exp(2i\pi k\ell/n)$ ($\ell \in \mathbb{Z}/n\mathbb{Z}$). La matrice de passage de l'une à l'autre est une matrice de Vandermonde, c'est ce que l'on appelle la transformée de Fourier discrète (TFD). Sur le plan conceptuel, c'est très simple, mais cela donne lieu à un des algorithmes les plus riches d'applications : la transformation de Fourier rapide (FFT), utile pour des calculs sophistiqués (images, analyse du signal) ou basiques (multiplication). Voir [67].

Prenons à présent $G = \mathbb{R}/\mathbb{Z}$, qui, à défaut d'être fini, est compact. Comme il est abélien, les représentations irréductibles de dimension finie de ce groupe sont de dimension 1. Connaissant les sous-groupes à un paramètre de $\mathrm{GL}_n(\mathbb{R})$ ($n \in \mathbb{N}$), on en déduit que les représentations continues de G sont les $\chi_\ell : \theta \mapsto \exp(2i\pi\ell\theta)$ ($\ell \in \mathbb{Z}$). La théorie des séries de Fourier donne des conditions sur une fonction pour qu'elle puisse s'écrire comme une somme (infinie cette fois) de la même forme que dans (F) : par exemple, être dans L^2.

Si maintenant, on prend $G = \mathbb{R}$, qui est au moins localement compact, les représentations irréductibles (unitaires de dimension finie) sont les $\chi_x : t \mapsto \exp(itx)$; il faut remplacer la somme par une intégrale pour obtenir une fonction comme combinaison linéaire (en un sens étendu) de caractères de $\mathbb{R}$, les coefficients étant donnés par la transformée de Fourier de la fonction. On a une interprétation analogue des transformées de Mellin pour $\mathbb{R}^{+*}$

(représentations non unitaires, de sorte que la transformation inverse est un peu différente) et de Laplace (bilatérale) pour le semi-groupe $\mathbb{R}^+$ (le groupe $\mathbb{R}^*$).

Il y a dans toutes ces situations un ingrédient implicitement présent depuis le début : l'idée d'une *mesure invariante*, une mesure sur le groupe invariante par translation.

théorie	groupe	caractères	mesure invariante
groupes finis	G fini	$\chi \in \mathrm{Irr}(G)$	$\frac{1}{\lvert G\rvert}\#$
TFD	$\mathbb{Z}/n\mathbb{Z}$	$k \mapsto e^{i2\pi\ell k/n}$ $(\ell \in \mathbb{Z}/n\mathbb{Z})$	$\frac{1}{n}\#$
séries de Fourier	$\mathbb{R}/\mathbb{Z}$	$\chi_\ell : \theta \mapsto e^{2i\pi\ell\theta}$ $(\ell \in \mathbb{Z})$	$\mathrm{d}\theta$
transformée de Fourier	$\mathbb{R}$	$\chi_x : t \mapsto e^{2i\pi xt}$ $(x \in \mathbb{R})$	$\mathrm{d}t$
Mellin	$\mathbb{R}^{+*}$	$\chi_x : u \mapsto u^x$ $(x \in \mathbb{R})$	$\frac{\mathrm{d}u}{u}$
Laplace	« $\mathbb{R}^+$ »	$\chi_x : t \mapsto e^{xt}$ $(x \in \mathbb{R})$	$\mathrm{d}t$

Ainsi, le théorème C.7 est un des avatars de l'idée très générale de Fourier : il est « naturellement bon » d'exprimer une fonction comme « combinaison linéaire » de coefficients matriciels (voir l'exercice F.12) ou une fonction centrale sur un groupe non abélien comme « combinaison linéaire » de caractères. Plus généralement, l'analyse harmonique consiste à décomposer des espaces de fonctions (continues, de carré intégrable...) sur un espace X sur lequel un groupe localement compact G agit comme somme (si possible directe, éventuellement infinie) de représentations simples de G.

La théorie fonctionne parfaitement pour les groupes *compacts*, qui donnent un cadre pour généraliser les groupes finis non commutatifs et $\mathbb{R}/\mathbb{Z}$. La décomposition de la représentation régulière devient le théorème de Peter-Weyl : les coefficients matriciels forment une base hilbertienne de l'espace des fonctions L^2, voir [76, §I-4]. Dans le livre [27], Jacques Faraut traite l'exemple de la sphère de dimension 2 : les « harmoniques sphériques » qui apparaissent sont essentiels pour la description quantique d'un atome d'hydrogène. La théorie pour les groupes de Lie non compacts est encore l'objet de recherches.

Au fond, on peut se demander si les représentations des groupes finis, c'est de l'analyse harmonique dans un contexte trivial sans analyse, ou si l'analyse harmonique, c'est essayer d'imiter à grand-peine la situation idéale des groupes finis... Gauss pensait-il à la fonction Γ d'Euler en formant les sommes qui portent son nom ?

D. Annexe. Algèbre de groupe

On introduit une algèbre qui joue dans cette théorie le même rôle que l'algèbre des polynômes pour la réduction des endomorphismes ou l'algèbre des chemins d'un carquois pour ses représentations ; encore une fois, le mot clé ici est « linéarisation ». Outre l'éclaircissement conceptuel qu'elle permet, l'étude de sa structure permet d'interpréter la relation numérique du corollaire C.5 et donne une deuxième preuve, plutôt plus simple, du corollaire C.8.

D.1. L'algèbre $\mathbb{K}G$

Dans ce paragraphe, $\mathbb{K}$ est un corps quelconque. On introduit un symbole δ_g pour chaque élément $g \in G$. Comme ci-dessus, on note $\mathbb{K}G$ l'espace des combinaisons linéaires formelles $\sum_{g\in G} a_g\delta_g$, où $a_g \in \mathbb{K}$ pour tout g. Notons que l'espace ambiant n'est toujours rien d'autre que l'espace $\mathbb{K}^G$, qui est isomorphe à $\mathbb{K}G$. On définit le produit de deux éléments de $\mathbb{K}G$ par :

$$\Big(\sum_{g\in G} a_g\delta_g\Big)\Big(\sum_{g\in G} b_g\delta_g\Big) = \sum_{h\in G}\Big(\sum_{gg'=h} a_g b_{g'}\Big)\delta_h.$$

On vérifie que $\mathbb{K}G$ est une algèbre associative et unitaire, dont le neutre est δ_e, où e est le neutre de G. On a en particulier :

$$\forall g, h \in G, \quad \delta_g\delta_h = \delta_{gh}.$$

D.2. Remarque. Il est raisonnable de penser $\mathbb{K}G$ comme l'espace des distributions sur G, qui s'identifie, pour un ensemble fini, à l'espace des fonctions[17] de G dans $\mathbb{C}$; alors δ_g s'interprète comme la fonction caractéristique de $\{g\}$, qui vaut 1 en g et 0 ailleurs, et le produit s'interprète comme le produit de convolution $*$:

$$\delta * \delta'(g) = \sum_{hk=g} \delta(h)\delta'(k).$$

Il est équivalent de se donner une représentation de G sur $\mathbb{K}$ et de se donner un *module* (à gauche, de dimension finie) sur l'algèbre $\mathbb{K}G$.

> D'une part, si $\rho : G \to \mathrm{GL}(V)$ est une représentation, $\mathbb{K}G$ agit sur V par :
> $$\forall (a_g) \in \mathbb{K}^G,\ \forall v \in V, \quad \Big(\sum_{g\in G} a_g\delta_g\Big)v = \sum_{g\in G} \rho(g)(v).$$
> Inversement, si V est un $\mathbb{K}G$-module, on pose $\rho(g)(v) = \delta_g \cdot v$ pour $g \in G$ et $v \in V$. Comme $\delta_g\delta_{g^{-1}} = \delta_e$ et que δ_e agit sur V comme l'identité, $\rho(g)$ appartient à $\mathrm{GL}(V)$. La relation $\delta_g\delta_h = \delta_{gh}$ montre que ρ est un morphisme.

[17] Pour être plus naturel, il vaudrait mieux identifier δ_g à la distribution de Dirac en g, qui est un élément du dual des fonctions.

On vérifie que ce dictionnaire se prolonge aux sous-représentations/sous-modules et aux morphismes de représentations/morphismes de modules.

En particulier, la *représentation régulière* est la représentation correspondant au $\mathbb{C}G$-module $\mathbb{C}G$ pour la multiplication à gauche.

D.3. Exemple. Soit, à nouveau, $G = \mathbb{Z}/n\mathbb{Z}$ un groupe cyclique, que l'on notera de façon multiplicative, et g un générateur. On suppose que $\mathbb{K} = \mathbb{C}$. Pour k compris entre 0 et $n-1$, soit $x^k = \delta_{g^k}$: on forme ainsi une base de $\mathbb{C}G$. Cette écriture permet d'identifier $\mathbb{C}G$ avec le quotient $\mathbb{C}[x]/(x^n - 1)$. Le lemme chinois donne alors :

$$\mathbb{C}G \simeq \bigoplus_{k=0}^{n-1} \mathbb{C}[x]/(x - \zeta^k), \quad \text{où } \zeta = e^{2i\pi/n}.$$

Si l'on compare à la décomposition de la proposition C.4, on voit que l'on a décomposé ici la représentation régulière $\mathbb{C}G$ en somme de représentations simples, toutes de dimension 1 et de multiplicité 1, correspondant aux n représentations irréductibles de G.

D.4. Structure de l'algèbre $\mathbb{C}G$

Nous avons vu dans la proposition C.4 une décomposition de la représentation $\mathbb{C}G$. Il n'est pas beaucoup plus difficile d'en obtenir une décomposition en tant qu'algèbre. Elle est donnée en terme d'algèbres de matrices. Commençons par un lemme utile[18].

D.5. Lemme. *L'intersection des annulateurs dans $\mathbb{C}G$ des représentations irréductibles d'un groupe fini G est nulle.*

Démonstration. Soit a dans $\mathbb{C}G$ tel que a annule toute représentation irréductible V_χ de G. Alors, par la proposition C.4, la multiplication à gauche par a annule $\mathbb{C}G$. En particulier, $a = a \cdot e = 0$. □

D.6. Proposition. *Soit G un groupe fini. Il existe un isomorphisme d'algèbres (non canonique)*

$$\Phi : \mathbb{C}G \to \bigoplus_{\chi \in \mathrm{Irr}(G)} \mathscr{M}_{\chi(e)}(\mathbb{C}).$$

Démonstration. Soit $V = \sum_{i \in \mathrm{Irr}(G)} S_i$. Le lemme qui précède assure que le morphisme d'algèbres $\Phi : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(V)$ associé à la représentation est injectif.

[18] Dans la botanique des lemmes, le lecteur avisé aura remarqué qu'il existe des lemmes « kleenex », qui ne servent qu'une fois, des lemmes « techniques », comprendre « laborieux ». Celui-ci est utile, agréable, et sert même très souvent.

En choisissant une base de $\mathbb{C}G$ adaptée à la décomposition de V ci-dessus, et en prenant les matrices dans cette base, l'image d'un élément par Φ_{reg} est diagonale par blocs. On obtient un nouveau morphisme injectif :

$$\Phi : \mathbb{C}G \to \bigoplus_{\chi \in \mathrm{Irr}(G)} \mathscr{M}_{\chi(e)}(\mathbb{C}).$$

D'après le corollaire C.5, on a égalité des dimensions, et Φ est donc un isomorphisme. □

Intéressons-nous un peu au centre $Z(G)$ de l'algèbre $\mathbb{C}G$.

D.7. Proposition. *Le centre $Z(G)$ de $\mathbb{C}G$ est une sous-algèbre de $\mathbb{C}G$, dont une base est donnée par les fonctions caractéristiques des classes de conjugaison de G. Sa dimension est donc $|\mathrm{Irr}(G)|$.*

Démonstration. Soit C_j une classe de conjugaison de G. Alors, les $z_j = \sum_{g \in C_j} \delta_h$ pour tout j, forment une famille, clairement libre, qui est bien dans $Z(G)$ puisque l'on a :

$$\forall h \in G, \quad \delta_h\Big(\sum_{g \in G} a_g \delta_g\Big) = \Big(\sum_{g \in G} a_g \delta_{hgh^{-1}}\Big)\delta_h$$

(prendre $a_g = 1$ si $g \in C_j$, et $a_g = 0$ sinon).

De plus, cette même formule montre que tout élément central est une combinaison linéaire des z_j. En effet, on obtient par identification que si $\sum_{g \in G} a_g \delta_g$ est central, alors a_g est constant sur les classes de conjugaison.□

D.8. Exercice

1. *Montrer que le centre de $\bigoplus_{\chi \in \mathrm{Irr}(G)} \mathscr{M}_{\chi(e)}(\mathbb{C})$ est $\bigoplus_{\chi \in \mathrm{Irr}(G)} \mathbb{C}\,\mathrm{Id}_{\chi(e)}$.*

   Le commutant de l'algèbre des matrices est la droite engendrée par l'identité.

2. *Déduire des deux propositions précédentes deux bases pour le sous-espace $Z(G)$ et ainsi, une preuve alternative du fait que G a autant de caractères complexes irréductibles que de classes de conjugaison.*

   Une base est (z_j), l'autre correspond aux composantes $\Phi^{-1}\big(\mathrm{Id}_{\chi(e)}\big)$.

3. *Les deux bases sont-elles identiques ?*

   Non, sauf si G est réduit à l'identité. On remarque que δ_e est un élément z_j où la classe de conjugaison C_j est réduite à l'élément neutre, et $\Phi(\delta_e)$ est l'identité $\bigoplus_{\chi \in \mathrm{Irr}(G)} \mathrm{Id}_{\chi(e)}$.

D.9. Idempotents centraux de $\mathbb{C}G$ et composantes isotypiques

Nous précisons la description de l'autre base de l'algèbre $Z(G)$ présentée dans l'exercice D.8 sous la forme d'idempotents centraux. Lorsque l'on applique la proposition A.21 à la représentation régulière, on obtient que l'élément[19]

$$\varepsilon = \frac{1}{|G|} \sum_{g \in G} \delta_g$$

est un idempotent de $\mathbb{C}G$ (et il est central) : en effet, la multiplication par ε est exactement la projection π pour $V = \mathbb{C}G$, d'où : $\varepsilon^2 = \varepsilon^2 \delta_e = \varepsilon \delta_e = \varepsilon$. Comme ε est central, l'idéal $\varepsilon\mathbb{C}G$ est bilatère et c'est aussi l'image de π, c'est-à-dire l'espace des invariants de $\mathbb{C}G$.

D.10. Exercice. *Montrer que l'image de cet idéal par le morphisme Φ de la proposition D.6 est l'algèbre de matrices $\mathscr{M}_{\dim V_j}(\mathbb{C})$ dont l'indice j correspond à la représentation triviale (de dimension 1).*

Remarquer que $\Phi(\varepsilon)$ est le morphisme π sur les invariants de V, c'est-à-dire sur la représentation simple et triviale S_j.

On peut encore étendre cela à d'autres caractères que le trivial. D'après le corollaire B.12 :

$$\varepsilon_\chi = \frac{\chi(e)}{|G|} \sum_{g \in G} \overline{\chi(g)} \delta_g$$

correspond via Φ à l'idempotent de $\bigoplus_{\chi' \in \mathrm{Irr}(G)} \mathscr{M}_{\chi'(e)}(\mathbb{C})$ dont la composante en χ' est $\mathrm{Id}_{\chi\chi'} \mathrm{Id}_{\chi(e)}$.

E. Annexe. Représentations sur un sous-corps de $\mathbb{C}$

E.1. Considérations générales

Dans la théorie élémentaire des représentations, il est commode de travailler avec des représentations complexes, c'est-à-dire des actions linéaires du groupe à l'étude sur des espaces vectoriels complexes ou, ce qui revient au même via le choix d'une base, des morphismes à valeurs dans $\mathrm{GL}_n(\mathbb{C})$ pour n entier. Mais il peut être intéressant de travailler sur des corps différents. Par exemple, l'isomorphisme $\mathrm{PSL}_2(\mathbb{F}_7) \xrightarrow{\sim} \mathrm{GL}_3(\mathbb{F}_2)$, voir corollaire VII-4.2, peut très légitimement être considéré comme une représentation du groupe $\mathrm{PSL}_2(\mathbb{F}_7)$ sur le corps à deux éléments !

[19] On a malencontreusement noté e le neutre de G, si bien que cette lettre traditionnelle pour les idempotents est proscrite.

Plus près des préoccupations de ce chapitre, si nous voulons utiliser la théorie des représentations pour construire des polyèdres dans $\mathbb{R}^3$, il faudra bien réussir à passer de $\mathbb{C}$ à $\mathbb{R}$ à un moment ou à un autre.

La théorie sur les complexes est particulièrement agréable, parce que $\mathbb{C}$ est un corps algébriquement clos de caractéristique 0. La théorie possède les mêmes vertus qu'en algèbre linéaire habituelle, lorsque l'on n'étudie qu'un seul endomorphisme à la fois.

Propriétés principales des représentations d'un groupe fini G (sur un corps donné $\mathbb{K}$) :

1. lemme de Schur (voir la proposition A.8 : le commutant $\mathrm{End}_{\mathbb{K}G}(V)$ d'une représentation irréductible V est un corps (non nécessairement commutatif) ; sous cette forme, cela reste vrai sur n'importe quel corps ;
2. semi-simplicité : toute représentation ρ (de dimension finie, bien sûr) est somme directe de représentations simples : cela est vrai sur n'importe quel corps de caractéristique 0, voir A.16 ;
3. le caractère d'une représentation la caractérise (si deux représentations ont le même caractère, elles sont isomorphes) : sur le corps des réels, au moins, c'est vrai (esquisse : on se ramène au cas de deux structures ρ et τ de représentations de G sur l'espace $\mathbb{C}$, telles que $\rho(g)$ et $\tau(g)$ sont des matrices réelles pour tout g avec une matrice P de $\mathrm{GL}_n(\mathbb{C})$ telle que $P\rho(g) = \tau(g)P$ pour tout g. Procéder ensuite comme pour [H2G2, proposition III-4.1] pour trouver une matrice Q dans $\mathrm{GL}_n(\mathbb{R})$ possédant la même propriété) ;
4. attention ! Une représentation $G \to \mathrm{GL}_n(\mathbb{K})$, où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, peut être simple, et considéré comme une représentation complexe via le plongement naturel $\mathrm{GL}_n(\mathbb{K}) \to \mathrm{GL}_n(\mathbb{C})$, elle devient en revanche réductible ; par exemple, la représentation
$$\rho : \mathbb{Z}/4\mathbb{Z} \to \mathrm{GL}_2(\mathbb{R}), \quad \bar{1} \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
où les générateurs agissent comme des rotations d'angle droit, est simple, mais la représentation définie de même sur $\mathbb{C}$ est somme de deux caractères linéaires (définis par $\bar{1} \mapsto \pm i$) ;
5. en revanche, si le caractère χ d'une représentation définie sur un sous-corps $\mathbb{K}$ de $\mathbb{C}$ satisfait à $\langle \chi, \chi \rangle = 1$, alors la représentation est irréductible sur $\mathbb{K}$ puisqu'irréductible sur $\mathbb{C}$;
6. de même que dans toute représentation complexe de G, il existe un produit scalaire hermitien invariant (lemme A.15, dans toute représentation réelle de G, il existe un produit scalaire euclidien invariant (esquisse : choisir un produit scalaire euclidien $(\cdot\,,\cdot)$ quelconque ; la forme suivante convient : $(u,v) \mapsto (u,v)_G = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} (g \cdot u, g \cdot v)$;

7. il y a autant de classes de conjugaison dans G que de classes d'isomorphisme de représentations complexes simples, voir le corollaire C.8 ; cela devient faux en général si l'on remplace $\mathbb{C}$ par un sous-corps ; par exemple, $\mathbb{Z}/4\mathbb{Z}$ a quatre classes de conjugaison mais seulement trois représentations irréductibles réelles : deux de degré 1 et une de degré 2, selon que l'on envoie $\bar{1}$ sur 1, -1 ou $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

E.2. Représentation par permutation sur un sous-corps $\mathbb{K}$ de $\mathbb{C}$

Soit G un groupe fini agissant sur un ensemble fini X. On associe à cette action une représentation par permutation définie sur $\mathbb{R}$ comme ci-dessus. Soit $\mathbb{K}X$ l'espace vectoriel muni de sa base canonique $(e_x)_{x\in X}$ indexée par X. On fait agir G de façon linéaire sur $\mathbb{K}X$ par :

$$\forall g \in G,\ \forall x \in X, \quad \rho_X(g)(e_x) = g \cdot e_x = e_{g\cdot x}.$$

La somme $s = \sum_{x\in X} e_x$ est invariante sous G, donc elle engendre une sous-représentation isomorphe à la représentation triviale. L'hyperplan V_X défini par l'annulation de la somme des coordonnées est un supplémentaire de $\mathbb{K}s$ stable sous G : c'est une sous-représentation de $\mathbb{K}X$ (isomorphe à $\mathbb{K}X/\mathbb{K}s$). Avec la proposition B.15 et la propriété 5 ci-dessus, on obtient le lemme suivant.

Lemme. *(Notations ci-dessus.) Si G agit deux fois transitivement sur X, alors V_X est irréductible sur $\mathbb{K}$.*

E.3. Réalisation réelle d'une représentation complexe

Le succès de la théorie des représentations doit beaucoup aux caractères, qui constituent un outil de simplification remarquable. Si V est une représentation de degré n du groupe fini G, on résume finalement la donnée de $|G|$ matrices (n, n) en la donnée de $\dim Z(G) = |\mathrm{Irr}(G)|$ scalaires (en fait, le nombre de classes de conjugaison), ce qui constitue une énorme économie de moyens. Toutefois, la théorie des caractères ne résout pas tout, voir par exemple le §2.1 sur la construction de l'icosaèdre. Il est donc intéressant de savoir ce que l'on peut lire, ou pas, sur la table des caractères d'un groupe. Un résultat inattendu est que l'on peut savoir, à partir de son caractère, si la représentation correspondante (unique à isomorphisme près) se réalise sur le corps des réels. Le résultat que nous allons montrer est étonnant et même, légèrement contre-intuitif : évidemment, si le caractère n'est pas à valeurs dans $\mathbb{R}$, on peut oublier l'idée de la représenter sur $\mathbb{R}$, mais une représentation irréductible pourra ne pas être réalisable sur $\mathbb{R}$ alors que son caractère est réel. Le critère permettant de différencier ces deux situations repose sur un calcul simple sur le caractère de la représentation.

Soit G un groupe fini et soit $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ une représentation matricielle de caractère χ. On dit que ρ (ou χ) se réalise sur $\mathbb{R}$ s'il existe une

représentation $\rho_0 : G \to \mathrm{GL}_n(\mathbb{R})$ telle que ρ soit isomorphe à $\iota \circ \rho_0$, où ι est l'injection naturelle $\mathrm{GL}_n(\mathbb{R}) \hookrightarrow \mathrm{GL}_n(\mathbb{C})$.

Bien sûr, pour que ρ se réalise sur $\mathbb{R}$, il est nécessaire que χ soit à valeurs réelles. L'exemple ci-dessous montre que ce n'est pas suffisant. Nous allons établir un critère pour caractériser les représentations qui se réalisent sur $\mathbb{R}$.

E.4. Exemple. Voici un contre-exemple célèbre qui nous rappelle au groupe quaternionique H_8. Nous avons déjà vu ce groupe dans [H2G2, chapitre VII] sur les quaternions et nous le rencontrerons à nouveau au §XI-8 sous le nom de $\tilde{D}_4$.

Soit $H_8 = \{\pm 1, \pm I, \pm J, \pm K\}$, le groupe quaternionique ($I^2 = J^2 = K^2 = IJK = -1$). Les matrices de Pauli, que l'on a déjà rencontrées dans [H2G2, chapitre VII], fournissent une représentation fidèle $\sigma : H_8 \to \mathrm{GL}_2(\mathbb{C})$:

$$\sigma(I) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \sigma(J) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \sigma(K) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

On voit en prenant les traces que le caractère de cette représentation est à valeurs réelles et, pourtant, elle ne peut pas se réaliser sur $\mathbb{R}$. En effet, si c'était le cas, on obtiendrait, via le choix d'un produit scalaire euclidien invariant par H_8, voir le §E, une injection $\rho_0 : H_8 \hookrightarrow \mathrm{O}_2(\mathbb{R})$. Comme la représentation est fidèle, on peut identifier H_8 et son image dans $\mathrm{O}_2(\mathbb{R})$. Soit $H_8^+ = H_8 \cap \mathrm{SO}_2(\mathbb{R})$, on a une injection

$$H_8/H_8^+ \hookrightarrow \mathrm{O}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Or, H_8/H_8^+ n'est pas le groupe trivial, sans quoi H_8 serait inclus dans $\mathrm{SO}_2(\mathbb{R})$, qui est abélien. Il existe donc un élément de H_8 qui n'est pas une rotation, c'est donc une symétrie orthogonale, d'ordre 2. Cela fait au moins deux éléments d'ordre 2 dans H_8, à savoir $-\mathrm{Id}$, qui est dans $\mathrm{SO}_2(\mathbb{R})$ et cette symétrie. Absurbe.

E.5. Proposition. *Soit G un groupe fini et soit $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ une représentation irréductible. On suppose que le caractère χ de ρ est à valeurs réelles. Les assertions suivantes sont équivalentes :*

(i) *la représentation ρ peut se réaliser sur $\mathbb{R}$;*

(ii) *il existe une forme bilinéaire symétrique non nulle sur $\mathbb{C}^n$ invariante*[20] *par G ;*

(iii) *on a :* $\dfrac{1}{|G|} \displaystyle\sum_{g \in G} \chi(g^2) = 1.$

[20] Si β est cette forme, on a : $\beta(\rho(g)u, \rho(g)v) = \beta(u, v)$ pour u, v de $\mathbb{C}^n$ et g de G.

Démonstration. Montrons d'abord que les assertions (i) et (ii) sont équivalentes. Supposons qu'il existe une réalisation réelle $\rho_0 : G \to \mathrm{GL}(E)$ de ρ, où E est un espace réel. L'espace de la représentation de ρ_0 est $E \simeq \mathbb{R}^n$. Soit $\langle \cdot, \cdot \rangle$ un produit scalaire euclidien sur $\mathbb{R}^n$ invariant par G (par exemple $\langle u, v \rangle = \sum_{g \in G} (\rho_0(g)u, \rho_0(g)v)$ pour u et v de $\mathbb{R}^n$, où $(\cdot, \cdot)$ est un produit scalaire euclidien arbitraire). Soit B la matrice de ce produit scalaire dans la base canonique. Elle est invariante par G : ${}^t\rho_0(g) B \rho_0(g) = B$ pour g de G.

On peut identifier l'espace complexifié $E_{\mathbb{C}}$ de $E \simeq \mathbb{R}^n$ à $\mathbb{C}^n$. Mais alors, la forme quadratique complexe ayant pour matrice B dans la base canonique de $\mathbb{C}^n$ est invariante par G : ${}^t\rho(g) B \rho(g) = B$ pour g de G.

Inversement, supposons qu'il existe β, une forme bilinéaire symétrique non nulle sur $\mathbb{C}^n$ invariante par G. Choisissons un produit scalaire hermitien $\langle \cdot, \cdot \rangle$ invariant par G (semi-linéaire par rapport à la première variable ; par exemple $\langle u, v \rangle = \sum_{g \in G} \big(\rho(g)u, \rho(g)v\big)$ pour u et v de $\mathbb{R}^n$, où $(\cdot, \cdot)$ est un produit scalaire hermitien arbitraire). Le noyau de β est stable par G et ρ est irréductible, donc β (qui est non nulle) est non dégénérée, puisque son noyau est une sous-représentation, distincte de $\mathbb{C}^n$ par hypothèse. Pour u de $\mathbb{C}^n$, il existe un unique $\varphi(u)$ dans $\mathbb{C}^n$ tel que :

$$\forall v \in \mathbb{C}^n, \quad \beta(u, v) = \langle \varphi(u), v \rangle.$$

Comme la forme β (resp. $\langle \cdot, \cdot \rangle$) est bilinéaire (resp. sesqui-linéaire) et non dégénérée, l'application $\varphi : \mathbb{C}^n \to \mathbb{C}^n$ ainsi définie est semi-linéaire et bijective ; en particulier, φ^2 est linéaire. Pour u et v de $\mathbb{C}^n$, on a, par symétrie de β :

$$\langle \varphi^2(u), v \rangle = \beta\big(\varphi(u), v\big) = \beta\big(v, \varphi(u)\big) = \langle \varphi(v), \varphi(u) \rangle,$$

d'où l'on tire encore, par symétrie hermitienne :

$$\langle \varphi^2(u), v \rangle = \langle \varphi(v), \varphi(u) \rangle = \overline{\langle \varphi(u), \varphi(v) \rangle} = \overline{\langle \varphi^2(v), u \rangle} = \langle u, \varphi^2(v) \rangle$$

(la troisième égalité n'est autre que la première où l'on a permuté u et v).

Ainsi, φ^2 est hermitien. L'égalité $\langle \varphi^2(u), u \rangle = \langle \varphi(u), \varphi(u) \rangle$, valable pour tout u, montre que φ^2 est défini positif.

Par ailleurs, comme les formes sont invariantes, φ est invariante : pour g de G et u, v de $\mathbb{C}^n$, on a :

$$\langle \rho(g)\varphi(u), v \rangle = \langle \varphi(u), \rho(g)^{-1} v \rangle = \beta\big(u, \rho(g)^{-1} v\big) = \beta\big(\rho(g)u, v\big) = \langle \varphi(\rho(g)u), v \rangle.$$

Comme v est quelconque, on en tire : $\rho(g) \circ \varphi = \varphi \circ \rho(g)$ pour tout g. Par le lemme de Schur, on a : $\varphi^2 = \lambda \mathrm{Id}$ pour λ convenable ; par positivité, λ est un réel strictement positif.

En identifiant $\mathbb{C}^n$ à l'espace vectoriel réel $\mathbb{R}^{2n}$, notons V_+ (resp. V_-) l'espace propre de φ associé à la valeur propre $\sqrt{\lambda}$ (resp. $-\sqrt{\lambda}$) : puisque φ est annulé par le polynôme $X^2 - \lambda$, ce sont deux sous-espaces réels supplémentaires de $\mathbb{C}^n$. Par semi-linéarité, pour v de $\mathbb{C}^n$, on a : $\varphi(iv) = -i\varphi(v)$, d'où l'on déduit que la multiplication par i échange V_+ et V_- ; en formule : $iV_+ = V_-$. Ainsi, V_+ et V_- ont la même dimension réelle n et, de plus, une base de l'espace vectoriel réel V_+ est aussi une base de $\mathbb{C}^n$. Enfin, comme φ commute avec $\rho(g)$ pour tout g de G, l'espace V_+ est stable par les $\rho(g)$. Conclusion : puisque le $\mathbb{C}$-espace engendré par V_+ est $E_{\mathbb{C}} = \mathbb{C}^n$, l'espace V_+ est un espace réel qui réalise ρ.

Reste à montrer l'équivalence avec (iii). Soit Ψ le caractère de G sur l'espace des formes bilinéaires symétriques sur V. Par la proposition B.21 (iv), la multiplicité du caractère trivial dans Ψ est au plus 1, et l'existence d'une forme invariante équivaut donc à la relation : $\langle \Psi, 1 \rangle = 1$.

Le calcul de Ψ est fait dans le lemme B.19. En remarquant que χ est à valeurs réelles et que $\chi(g^{-1}) = \overline{\chi(g)}$ pour tout g de G, on peut écrire :

$$\langle \Psi, 1 \rangle = \frac{1}{|G|} \sum_{g \in G} \frac{\chi(g^{-2}) + \chi(g)^{-2}}{2} = \frac{1}{|G|} \sum_{g \in G} \frac{\chi(g^2) + \chi(g)^2}{2}.$$

(On aurait aussi pu appliquer la proposition B.21 (i) à V^*.)

La valeur moyenne de χ^2 est le produit scalaire de caractères $\langle \overline{\chi}, \chi \rangle$. Comme χ est à valeurs réelles et irréductible, il vient : $\langle \overline{\chi}, \chi \rangle = \langle \chi, \chi \rangle = 1$. On en déduit :

$$\frac{1}{|G|} \sum_{g \in G} \chi(g^2) = \frac{2}{|G|} \sum_{g \in G} \operatorname{tr} \Psi(g) - \frac{1}{|G|} \sum_{g \in G} \chi(g)^2 = 2\langle 1, \operatorname{tr} \circ \Psi \rangle - 1.$$

D'après la proposition B.21 (iv), cette somme vaut donc 1 si la représentation triviale apparaît dans $S^2\check{\rho}$ et -1 sinon. Les assertions (ii) et (iii) de la proposition sont donc équivalentes. □

On termine en beauté par un critère limpide pour détecter les représentations qui admettent une réalisation réelle.

E.6. Théorème. *Soit χ le caractère d'une représentation complexe irréductible V de G, on a :*

$$\frac{1}{|G|} \sum_{g \in G} \chi(g^2) = \begin{cases} 0 & \text{si } \chi \text{ n'est pas à valeurs réelles,} \\ 1 & \text{si } \chi \text{ est à valeurs réelles et réalisable sur } \mathbb{R}, \\ -1 & \text{si } \chi \text{ est à valeurs réelles mais pas réalisable sur } \mathbb{R}. \end{cases}$$

E.7. Remarque. Il est bon de rappeler ici que toute cette affriolante théorie des caractères repose sur le lemme de Schur et son interprétation en termes de formes hermitiennes. Bref, on ne peut se passer de travailler sur le corps des complexes. Le caractère, aussi réel soit-il, de la représentation d'un groupe G calculera la trace de matrices *a priori* complexes. Le problème principal, ici, est bien de déterminer si un caractère réel est, ou non, le caractère d'une représentation de G dans $\mathrm{GL}_n(\mathbb{R})$.

Démonstration. On remarque tout d'abord que si V est une représentation complexe de G, de caractère χ_V, on a alors :

$$\frac{1}{|G|}\sum_{g\in G}\chi_V(g) = \langle \chi_{\mathrm{triv}}, \chi_V\rangle = \dim V^G,$$

où χ_{triv} désigne le caractère de la représentation triviale. Posons alors :

$$a = \frac{1}{|G|}\sum_{g\in G}\frac{\chi(g)^2-\chi(g^2)}{2}, \quad s = \frac{1}{|G|}\sum_{g\in G}\frac{\chi(g)^2+\chi(g^2)}{2},$$
$$r = s-a = \frac{1}{|G|}\sum_{g\in G}\chi(g^2), \quad t = s+a = \frac{1}{|G|}\sum_{g\in G}\chi(g)^2.$$

Ainsi, a (resp. s) est la dimension de l'espace des formes alternées (resp. symétriques) G-invariantes. En particulier, ce sont des entiers positifs (ou nuls). De même, t est égal à $\dim \mathrm{Hom}(V^*, V)^G$, c'est-à-dire la dimension de l'espace des morphismes de représentations de V^* vers V. Comme ces deux représentations sont irréductibles, le lemme de Schur entraîne que t vaut 1 si V^* et V sont isomorphes et 0 sinon.

Or, les représentations V et V^* sont isomorphes si et seulement si leurs caractères coïncident, c'est-à-dire si $\chi = \overline{\chi}$, ce qui équivaut à dire que χ est réel.

Supposons donc que χ n'est pas à valeurs dans $\mathbb{R}$. Alors, t est nul et donc a et s le sont aussi, puisque a et s sont positifs (dimension oblige !) et de somme t. Ainsi, r est également nul.

Supposons que χ soit à valeurs dans $\mathbb{R}$ et la représentation se réalise sur $\mathbb{R}$. Alors, $r = 1$ par la proposition E.5.

Supposons que χ soit à valeurs dans $\mathbb{R}$ et la représentation ne se réalise pas sur $\mathbb{R}$. Alors, $r \neq 1$ par la proposition E.5. Comme $a + s = 1$, la seule possibilité est $a = 1$, $s = 0$ et donc $r = -1$. □

E.8. Conclusion

On peut essayer de faire le point sur la possibilité de réalisation réelle d'une représentation complexe de G. On a vu que si une représentation irréductible (complexe) V peut se réaliser sur $\mathbb{R}$, alors, il existe une forme

bilinéaire symétrique G-invariante, et de surcroît, définie positive, donc non nulle. Rien d'étonnant à cela, sinon que la réciproque reste vraie : l'existence d'une forme symétrique G-invariante implique une réalisation réelle de la représentation ! Or, si l'on connaît le caractère d'une représentation W, on sait calculer la dimension de ses invariants : $\dim W^G = \langle \chi_{\text{triv}}, \chi_W \rangle$. On applique alors ce résultat lorsque W est l'espace des formes bilinéaires symétriques sur V.

Ce résultat est déjà très honorable, mais un résultat plus général est alors à portée de main. Partons de la remarque anodine que si V possède une réalisation réelle, alors son caractère est réel. On est en droit de se demander si la réciproque est vraie. Réciproquement, donc, un caractère réel implique que V^* et V sont isomorphes, avec, par le lemme de Schur, $\dim \mathrm{Hom}(V^*, V)^G = 1$ (et un caractère non réel impliquerait de même que cette valeur est nulle). Si l'on se souvient ([H2G2, V-A.1]) de l'isomorphisme canonique, dont on vérifie qu'il commute à l'action de G, entre $\mathrm{Hom}(V^*, V)$ et l'espace des formes bilinéaires sur V, on obtient l'existence d'une *forme bilinéaire G-invariante*, unique à scalaire près, sur V. Mais, cette unique droite doit choisir entre être symétrique (c'est gagné !) ou antisymétrique (c'est perdu !), puisque la décomposition des formes selon leur symétrie est une décomposition de représentations. C'est aux formules de caractères d'en décider, via l'indicateur de Frobenius-Schur.

E.9. Définition (Indicateur de Frobenius-Schur). Soit χ le caractère d'une représentation complexe irréductible V de G. On dit que V est :

- *complexe* si $\frac{1}{|G|}\sum_{g\in G}\chi(g^2) = 0$,
- *réelle* si $\frac{1}{|G|}\sum_{g\in G}\chi(g^2) = 1$,
- *quaternionique* si $\frac{1}{|G|}\sum_{g\in G}\chi(g^2) = -1$.

L'entier $|G|^{-1}\sum_{g\in G}\chi(g^2)$ est appelé *indicateur* (ou *indicatrice* si l'on préfère rouler au féminin[21]) *de Frobenius-Schur*.

Reste un dernier mystère : pourquoi le troisième cas est-il appelé quaternionique ? L'exercice F.32 montre que dans ce cas, le G-module V peut être muni d'une structure de $\mathbb{H}$-module compatible avec la structure de G-module : autrement dit, on a un morphisme injectif de l'algèbre des quaternions $\mathbb{H}$ vers $\mathrm{End}(V)$ et tout élément de l'image de $\mathbb{H}$ commute à l'action de G (en fait, l'image est même égale au commutant de l'action de G).

[21] It's a free country!

F. Exercices du chapitre X

F.1. Exercice (Représentations continues du groupe $\mathbb{R}$)

1. *Montrer que toute représentation continue du groupe topologique* $\mathbb{R}$, i.e. *tout morphisme continu* $\mathbb{R} \to \mathrm{GL}_n(\mathbb{R})$ *ou* $\mathbb{R} \to \mathrm{GL}_n(\mathbb{C})$, *est de la forme* $t \mapsto \exp(tX)$ *pour une matrice* X *convenable.*

   Si f est un morphisme continu, alors f est dérivable, voir la preuve [H2G2, proposition IX-A.6.1] ; en dérivant en x l'égalité $f(x+y) = f(x)f(y)$, puis en prenant $x = 0$, on obtient une équation différentielle familière avec $X = f'(0)$.

2. *En déduire que toute représentation continue irréductible du groupe* $\mathbb{R}$ *sur le corps des complexes est de degré* 1.

   Trigonaliser X et en déduire une sous-représentation de degré 1.

3. *Exhiber une représentation continue sur* $\mathbb{C}$ *du groupe* $\mathbb{R}$ *qui n'est pas irréductible, mais n'est pas la somme directe de deux représentations irréductibles.*

   En dimension 2 : prendre une matrice X la plus simple possible qui ne soit pas diagonalisable sur $\mathbb{C}$. Voir aussi l'exercice F.46.

F.2. Exercice. *Soit* $\rho : G \to \mathrm{GL}(V)$ *une représentation d'un groupe* G *et soit* W *une sous-représentation de* V. *On fixe une base* $(e_1, \dots, e_m)$ *de* W *que l'on complète en une base* $\mathbf{e} = (e_1, \dots, e_n)$ *de* V.

1. *Montrer (ou plutôt remarquer) que la matrice de* $\rho(g)$ *dans la base* $\mathbf{e}$ *est triangulaire par blocs pour tout* g *de* G. *On notera donc*

$$\rho(g) = \begin{pmatrix} A(g) & X(g) \\ 0 & B(g) \end{pmatrix}.$$

2. *Soit* $\sigma : G \to \mathrm{GL}(V/W)$ *la représentation-quotient et posons* $\overline{v}$ *l'image d'un vecteur* v *de* V *dans* V/W. *Montrer (ou plutôt remarquer) que la matrice de* $\sigma(g)$ *dans la base* $(\overline{e_{m+1}}, \dots, \overline{e_n})$ *est* $B(g)$.

(Comparer à l'exercice II-A.5.)

Représentations de groupes abéliens

F.3. Exercice (Représentations d'un groupe cyclique)

Montrer que les représentations irréductibles du groupe additif $\mathbb{Z}/n\mathbb{Z}$ *sont les* $\rho_\omega : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$, $\rho_\omega(\bar{k}) = \omega^k$, *où* ω *est une racine* n*-ième de l'unité.*

F.4. Exercice (Algèbre d'un groupe cyclique)

Soit n un entier naturel strictement positif, soit $G = \mathbb{Z}/n\mathbb{Z}$, soit g un générateur de G et soit ζ une racine primitive n-ième de l'unité dans $\mathbb{C}$. Le morphisme d'algèbres défini par $\mathbb{C}[X] \to \mathbb{C}G$, $X \mapsto g$ identifie $\mathbb{C}[X]/(X^n - 1)$ à l'algèbre de groupe $\mathbb{C}G$.

1. *À l'aide du lemme des restes chinois, montrer que $A = \mathbb{C}[X]/(X^n - 1)$ possède n idempotents e_k $(0 \leqslant k \leqslant n-1)$ avec un isomorphisme d'anneaux $e_k A \simeq \mathbb{C}[X]/(X - \zeta^k)$.*
2. *En déduire que $\mathbb{C}G$ possède n idempotents e_k $(0 \leqslant k \leqslant n-1)$, que $\mathbb{C}Ge_k$ est une sous-représentation de $\mathbb{C}G$ de dimension 1. Montrer que l'on a un isomorphisme de représentations :*

$$\mathbb{C}G \simeq \bigoplus_{k=0}^{n-1} \mathbb{C}Ge_k.$$

   Considérer les éléments e_k de $\mathbb{C}G$ correspondant à $(0, \ldots, 1, \ldots, 0)$ via l'isomorphisme du lemme chinois.
3. *Expliciter la matrice de passage de la base $(\delta_{g^k})_{0 \leqslant k \leqslant n-1}$ à la base (e_k).*
   Noter que $\delta_g = \sum_k \zeta^k e_k$.
4. *On note $V_k = \mathbb{C}Ge_k$. Montrer que les V_k forment une famille complète de représentations irréductibles de G. Calculer le caractère χ_k de V_k. Reconnaître la matrice de la table de caractères de G et retrouver la formule $T^*T = n\,\mathrm{Id}$.*

Cet exercice nous a été suggéré par Robert Bonnet.

F.5. Exercice (Représentations des groupes finis abéliens)

Soit G un groupe fini abélien.

1. *Montrer que toute représentation irréductible complexe de G est de dimension 1.*
   Toute représentation de G provient de la donnée de matrices complexes diagonalisables qui commutent entre elles. On pense donc naturellement au théorème de diagonalisation simultanée.
2. A contrario, *donner une représentation de $\mathbb{Z}/4\mathbb{Z}$ de dimension 2 qui est irréductible sur $\mathbb{R}$.*
   Faire agir $\bar{1}$ par la matrice $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.
3. *En utilisant la classification des groupes abéliens de type fini, donner une description des représentations irréductibles de G.*
   Utiliser l'exercice F.22 et les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ pour construire $|G|$ représentations distinctes de degré 1 (forcément irréductibles) de G.

4. *Montrer que l'ensemble des morphismes de G vers $\mathbb{C}$ est un groupe $\widehat{G}$ pour la multiplication des fonctions et que ce groupe est isomorphe à G.*

   On montrera que $\widehat{\mathbb{Z}/n\mathbb{Z}}$ est (non canoniquement) isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et l'on exhibera un isomorphisme naturel de $\widehat{G} \times \widehat{H}$ vers $\widehat{G \times H}$.

5. *Exhiber un isomorphisme naturel de G vers $\widehat{\widehat{G}}$.*

   S'inspirer de la preuve de l'isomorphisme entre un espace de dimension finie et son bidual.

6. *Donner une preuve élémentaire du théorème C.7 dans le cas abélien.*

F.6. Exercice (Caractères de degré 1, groupe abélien)

Montrer que si tous les caractères irréductibles d'un groupe fini G sont de degré 1, alors G est abélien.

On a vu que $\bigoplus_{i\in \mathrm{Irr}(G)} S_i$ est une représentation fidèle de G (car la représentation régulière l'est !). Ainsi, G peut s'injecter comme sous-groupe de $\mathrm{Aut}\big(\bigoplus_{i\in \mathrm{Irr}(G)} S_i\big)$, qui par le lemme de Schur est une algèbre de matrices diagonales. Donc, G est abélien.

F.7. Exercice (Pourquoi faire simple ?)

En utilisant le fait que $4 = 1^2+1^2+1^2+1^2$ est la seule décomposition de 4 en somme de carrés contenant 1^2, montrer que tout groupe d'ordre 4 est abélien.

L'utilisation de l'exercice F.6 conjoint au fait que l'on a toujours la représentation triviale tue ce moustique à l'aide d'un outil de haute sophistication.

Lemme de Schur

F.8. Exercice (Private joke)

Qui n'a pas rencontré sur son chemin la matrice

$$A(a,b) = \begin{pmatrix} a & \dots & b \\ \vdots & \ddots & \vdots \\ b & \dots & a \end{pmatrix} \in \mathscr{M}_n(\mathbb{C})$$

à diagonaliser (pour un entier $n > 1$) ? Il suffit pour cela de diagonaliser la matrice $J = A(1,1)$, ce qui est facile, car son rang est 1 et sa trace est n. On obtient alors que $A(a,b) = (a-b)\mathrm{I}_n + bJ$ est diagonalisable ; ses valeurs propres sont $a-b$, avec multiplicité $n-1$, et $a+(n-1)b$ avec multiplicité 1. Nous proposons d'établir ce résultat avec une méthode moins simple, mais bien plus instructive, et avec la théorie des représentations !

1. *On considère l'action naturelle de $\mathfrak{S}_n$ sur $X = \{1, \dots, n\}$ et la représentation de $\mathfrak{S}_n$ sur $\mathbb{C}X$, voir B.14, qui en résulte. Montrer que $\mathbb{C}X$ se décompose en somme de deux représentations irréductibles non isomorphes.*

   Cela résulte directement de la proposition B.15.

2. *En déduire que l'algèbre des endomorphismes de représentations de $\mathbb{C}X$ est de dimension 2 et l'identifier à l'espace des matrices $A(a,b)$, $a, b \in \mathbb{C}$.*

   Toute matrice $A(a,b)$ commute avec toute matrice de permutation.

3. *Conclure.*

   Le lemme de Schur prouve que les deux sous-représentations irréductibles sont les deux sous-espaces propres annoncés. Les valeurs propres s'en déduisent à l'aide de traces.

F.9. Exercice (Un corps non-commutatif d'endomorphismes)

Encore une fois, le groupe quaternionique va nous donner un exemple où l'algèbre des endomorphismes d'une représentation irréductible est un corps non commutatif. Voir aussi F.32 pour une analyse plus générale.

Soit $H_8 = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$, le groupe quaternionique (on rappelle que le produit est donné par : $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{1}$).

1. *On considère la représentation complexe (voir [H2G2, §VII-1.3]) :*

$$\rho : H_8 \to \mathrm{GL}_2(\mathbb{C}), \quad \mathbf{i} \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

2. *Soit (e_1, e_2) la base canonique de $\mathbb{C}^2$. La famille (e_1, ie_1, e_2, ie_2) est une base d'un $\mathbb{R}$-espace vectoriel noté V. Montrer que la représentation ρ définit une représentation de degré 4 sur $\mathbb{R}$, et écrire les matrices décrivant l'action de $\mathbf{i}$, $\mathbf{j}$ et $\mathbf{k}$.*

3. *Montrer que l'algèbre des endomorphismes de cette représentation est de dimension 4 sur $\mathbb{R}$ et qu'elle est isomorphe au corps non commutatif des quaternions. Autrement dit, avec un léger abus :*

$$\mathrm{End}_{\mathbb{R}H_8}(V) \simeq \mathbb{H} \quad \textit{et} \quad \mathrm{End}_{\mathbb{C}H_8}(V) \simeq \mathbb{C}.$$

   Pour commuter à l'action de H_8, il suffit de commuter à celle de $\mathbf{i}$ et $\mathbf{j}$. On pourra résoudre une équation matricielle par blocs. Plus astucieusement, on pourra aussi utiliser [H2G2, remarque VII-1.3.1] sur la multiplication à gauche et à droite dans $\mathbb{H}$: le corps non commutatif $\mathbb{H}$ agit par multiplication à droite sur $\mathbb{H}$ et cette action commute à l'action de $\mathbf{i}$ et $\mathbf{j}$ à gauche.

4. *Montrer que la représentation réelle V est irréductible.*

   Exploiter « la » réciproque du lemme de Schur de la remarque A.10.

F.10. Exercice. *Soit G un groupe fini et soit $Z(G)$ son centre. On considère une représentation irréductible $\rho : G \to \mathrm{GL}(V)$ de degré $\dim_{\mathbb{C}}(V) = d$. On se propose de démontrer la formule*

$$\frac{1}{|Z(G)|} \sum_{z \in Z(G)} |\chi_\rho(z)|^2 = d^2,$$

où χ_ρ désigne le caractère de ρ.

1. *Montrer que, pour tout z de $Z(G)$, $\rho(z)$ est une homothétie de rapport $\lambda(z)$ non nul, et que $\lambda : Z(G) \to \mathbb{C}^*$ est un morphisme de groupes.*

   C'est le lemme de Schur. Le fait d'avoir un morphisme de groupes provient du fait que ρ est un morphisme.

2. *En déduire que V, vu comme représentation de $Z(G)$, est isomorphe à $d\mathbb{C}_\lambda$, c'est-à-dire la somme directe de d copies de $\mathbb{C}_\lambda$, où $\mathbb{C}_\lambda$ est la représentation de degré 1 de $Z(G)$ correspondant au morphisme λ.*

3. *Conclure.*

   Prendre la norme $Z(G)$-invariante de la représentation V restreinte au centre $Z(G)$.

F.11. Exercice (Calcul de la moyenne des matrices élémentaires)

Soit G un groupe fini et soient $\rho : G \to \mathrm{GL}(V)$ et $\rho' : G \to \mathrm{GL}(V')$ deux représentations irréductibles *complexes de G. On choisit une base (e_i) de V et une base (e'_k) de V' et l'on définit pour tous i et k deux morphismes f_{ik} et $\overline{f}_{ik}$ de $\mathrm{Hom}_{\mathbb{C}}(V, V')$ par leurs valeurs en un vecteur $v \in V$:*

$$f_{ik}(v) = e_i^*(v) e'_k,$$
$$\overline{f}_{ik}(v) = \frac{1}{|G|} \sum_{g \in G} \rho'(g)\Big(f_{ik}\big(\rho(g^{-1})(v)\big)\Big),$$

où (e_i^*) désigne comme d'habitude la base duale de (e_i).

1. *Montrer que $\overline{f}_{ik}$ est un morphisme de représentations de V vers V'.*

2. *En déduire que $\overline{f}_{ik}$ est nulle si V et V' sont non isomorphes.*

3. *On suppose que $V' = V$ de degré d, que $(e_i) = (e'_k)$ et $\rho' = \rho$. Montrer que l'on a : $\overline{f}_{ik} = \frac{1}{d}\delta_{ik}\,\mathrm{Id}_V$.*

   Par le lemme de Schur, $\overline{f}_{ik} = \lambda_{ik}\,\mathrm{Id}_V$ pour un λ dans $\mathbb{C}$. On a $d\lambda_{ik} = \mathrm{tr}(\overline{f}_{ik}) = \sum_j e_j^*\big(\overline{f}_{ik}(e_j)\big)$. On développera $\overline{f}_{ik}$ et l'on remarquera que la relation $\rho(g^{-1})\rho(g) = \rho(e)$ implique après écriture matricielle la formule :

$$\sum_j e_i^*\big(\rho(g^{-1})e_j\big) e_j^*\big(\rho(g)e_k\big) = \rho(e)_{ik} = \delta_{ik}.$$

F.12. Exercice (Relations d'orthogonalité pour les coefficients matriciels). *On considère l'espace $\mathbb{C}G$ vu comme espace des fonctions de G dans $\mathbb{C}$, voir remarque D.2. On munit alors $\mathbb{C}G$ d'une structure hermitienne par*

$$\langle f\,,f'\rangle = \frac{1}{|G|}\sum_{g\in G}\overline{f(g)}f'(g).$$

Pour tout ℓ dans $\mathrm{Irr}(G)$, on fixe une forme hermitienne G-invariante (on sait faire) sur le G-module simple S_ℓ, et une base $\mathbf{e}^\ell = (e_i^\ell)_{1\leqslant i\leqslant \dim S_\ell}$ de S_ℓ. Soit ρ^ℓ la représentation de G correspondante et ρ_{ij}^ℓ la fonction qui à tout g de G associe le coefficient d'indice (i,j) de $\rho^\ell(g)$ dans la base $\mathbf{e}^\ell$.

1. *Montrer que $\rho_{ij}(g^{-1}) = \overline{\rho_{ji}(g)}$.*
   La base a été choisie pour que la matrice de $\rho(g)$ soit hermitienne.
2. *Montrer en utilisant le morphisme Φ de la proposition D.6 que les ρ_{ij}^ℓ ($1\leqslant \ell\leqslant \mathrm{Irr}(G)$, $1\leqslant i,j\leqslant \dim S_\ell$) forment une base de $\mathbb{C}G$.*
3. *Exprimer $\rho_{ij}^\ell(g)$ en fonction de $\rho^\ell(g)$, de la base $\mathbf{e}^\ell$ et de sa base duale, puis, déduire de l'exercice F.11 que*

$$\left\langle \rho_{ij}^\ell, \rho_{i'j'}^{\ell'}\right\rangle = \begin{cases} \dfrac{1}{\dim S_\ell} & \text{si } i=j',\ j=i' \text{ et } \ell=\ell', \\ 0 & \text{sinon.}\end{cases}$$

F.13. Exercice (Réciproque du lemme de Schur)

Soient G un groupe fini et V un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et soit $\rho : G\to \mathrm{GL}(V)$ une représentation. On suppose que l'algèbre D des endomorphismes de V est une algèbre à division, i.e. *un corps, commutatif ou non.*

1. *On suppose que la caractéristique de $\mathbb{K}$ et le cardinal de G sont premiers entre eux. Montrer que V est irréductible.*
   Si V est réductible, utiliser la semi-simplicité et exhiber un élément de D non nul et non inversible avec des matrices par blocs.
2. *Donner un exemple où la caractéristique de $\mathbb{K}$ divise le cardinal de G et où V n'est pas irréductible.*
   Faute d'inspiration, consulter l'exercice F.47.

F.14. Exercice. *On précise ici certaines propriétés de la structure quaternionique. On suppose donc le $\mathbb{C}$-espace V muni d'une part, d'une structure de G-module irréductible et d'autre part d'une structure de $\mathbb{H}$-module, l'action de G commutant à l'action de $\mathbb{H}$. On note donc φ le morphisme non nul d'algèbres de $\mathbb{H}$ dans $\mathrm{End}(V)$ correspondant, ρ le morphisme de groupes $G\to \mathrm{GL}(V)$, et l'on suppose $\rho(g)\circ\varphi(h) = \varphi(h)\circ\rho(g)$ pour tout g de G et h de $\mathbb{H}$.*

1. *Montrer que φ est injectif.*
   Cela provient juste du fait que $\mathbb{H}$ est un corps.
2. *Montrer que le commutant de $\rho(G)$ dans $\mathrm{End}(V)$ est exactement $\varphi(\mathbb{H})$.*
   Comme V est irréductible, le lemme de Schur dit que ce commutant est un corps. Or, il contient $\varphi(\mathbb{H})$ et est de dimension finie. Il est connu que $\mathbb{H}$ n'a pas de surcorps de dimension finie autre que lui-même.

F.15. Exercice. *Encore une fois, ρ est une représentation de degré n, irréductible de G sur l'espace complexe V, mais dans la classification de la définition E.9, le type est réel. On a donc, voir preuve de la proposition E.5, une représentation $\rho_0 : G \to \mathrm{GL}(V_+)$ sur un espace réel V_+ de dimension n. Montrer que le commutant de $\rho_0(G)$ est $\mathbb{R}$.*

Le commutant de $\rho(G)$ est $\mathbb{C}$. Plus précisément, $\mathbb{R}$ stabilise V_+ et $i\mathbb{R}$ échange V_+ et V_-.

Botanique des représentations

F.16. Exercice (Deux groupes avec la même table des caractères)

Montrer que H_8 et D_4 ont la même table des caractères alors qu'ils ne sont pas isomorphes.

Par exemple, on peut voir qu'ils ont tous deux cinq classes de conjugaison et sont d'ordre 8. Cela implique quatre représentations de degré un et une de degré deux. Pour chaque groupe, les représentations de degré un se calculent facilement et la dernière s'en déduit par l'exercice C.14 ou la remarque qui le suit.

F.17. Exercice (Table des caractères des groupes non abéliens d'ordre 8)

À la fois récréatif et jubilatoire, l'exercice qui suit montre sans l'utilisation de la classification des groupes d'ordre 8, *que tous les groupes non abéliens d'ordre 8 ont la même table des caractères. Soit G un tel groupe.*

1. *Montrer que G possède au moins un caractère de degré strictement supérieur à 1.*
   C'est l'exercice F.6.
2. *En déduire que G possède quatre caractères de degré 1 et un de degré 2.*
   Il suffit de résoudre l'équation $n_1^2 + \cdots + n_k^2 = 8$ (les n_i ainsi que k étant des inconnues entières strictement positives) sachant qu'un des n_i vérifie $n_i > 1$ et qu'au moins un des n_i vaut 1, correspondant à la représentation triviale.
3. *En déduire que G possède cinq classes de conjugaison.*

4. *Montrer que le centre $Z(G)$ de G vérifie $Z(G) \simeq \mathbb{Z}/2\mathbb{Z}$ et $G/Z(G) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

   On utilise qu'un p-groupe possède un centre non trivial et que si le quotient de G par $Z(G)$ était cyclique, alors G serait abélien.

5. *Montrer que les quatre représentations de degré 1 de G proviennent des caractères du quotient $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

   Les représentations de degré 1 de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ se relèvent en des représentations distinctes de degré 1 de G, via la surjection canonique.

6. *Conclure que tous les groupes non abéliens d'ordre 8 ont même table des caractères.*

   Il ne reste maintenant qu'à montrer que la dernière ligne de la table de G, correspondant à la représentation de degré 2, est déterminée. Elle l'est par orthogonalité de la table des caractères, voir le corollaire C.12.

7. *Voyez-vous une façon de différencier les groupes H_8 et D_4, une fois ces groupes connus, via la table des caractères ?*

   L'indicateur de Frobenius-Schur fait toute la différence.

F.18. Exercice (Représentations du groupe du cube)

À rebours de la ligne directrice du chapitre (de la table des caractères à la réalisation comme groupe de symétrie d'un polyèdre), on construit la table des caractères du groupe G des isométries d'un cube en quelques coups de cuillère à pot.

1. *Construire, grâce à l'action de G sur les quatre diagonales du cube, un caractère irréductible de degré 3.*
2. *Construire, grâce à l'action de G sur les trois belles paires de faces opposées, un caractère irréductible de degré 2.*
3. *Construire, grâce à l'action de G sur les deux tétraèdres inscrits dans le cube, un caractère non trivial de degré 1.*
4. *Construire, grâce à l'action de G sur le cube, le caractère trivial.*
5. *Retrouver le caractère irréductible manquant comme produit de deux des caractères précédents. Pourquoi ne peut-on pas l'obtenir comme représentation par permutation ?*

Algèbre d'un groupe

F.19. Exercice. *Soit G un groupe fini et soit ρ une représentation complexe de G telle que son caractère χ s'annule pour tout $g \neq e$ (non neutre) de G. Montrer que le caractère χ est un multiple entier du caractère de la représentation régulière de G.*

On a d'une part $\langle \chi, \chi_{\text{triv}} \rangle = \chi(e)/|G|$, qui est entier, puisqu'il représente la multiplicité du caractère trivial dans ρ. D'autre part, pour tout caractère irréductible χ_i, on a $\langle \chi, \chi_i \rangle = \big(\chi(e)/|G|\big)\chi_i(e)$. Cela donne le résultat.

F.20. Exercice. *Soit $G = \mathfrak{S}_3$ le groupe symétrique sur trois lettres. Expliciter l'isomorphisme de la proposition C.5 entre $\mathbb{C}G$ et le produit d'algèbres $\mathbb{C} \oplus \mathbb{C} \oplus \mathscr{M}_2(\mathbb{C})$.*

F.21. Exercice. *On montrera que l'algèbre de Hecke $\mathscr{H}_{q,n}$, définie en I-5, est une « déformation » de l'algèbre du groupe $\mathfrak{S}_n$ sur $\mathbb{Q}$.*

1. *Montrer qu'il existe une unique famille de polynômes $Q_{w,w'}^{w''} \in \mathbb{Z}[X]$ telle que pour tout q, on ait*

$$T_w * T_{w'} = \sum_{w''} Q_{w,w'}^{w''}(q)\, T_{w''}\,.$$

   On fixe w' et l'on procède par récurrence sur la longueur de w en partant des formules donnant $T_s * T_{w'}$ pour toute transposition simple s. Le polynôme ne dépend pas de q, et comme il y a une infinité de q possibles (les puissances de nombres premiers), on a unicité du polynôme.

2. *Montrer que l'on peut définir une structure d'algèbre associative $\mathscr{H}_n$ sur le $\mathbb{Q}[X]$-module libre $\mathbb{Q}[X]^{\mathfrak{S}_n}$ de base canonique $(T_w)_{w \in \mathfrak{S}_n}$ par*

$$T_w * T_{w'} = \sum_{w''} Q_{w,w'}^{w''}(X)\, T_{w''}.$$

   Il suffit de montrer l'associativité. Elle se ramène à l'annulation d'une certaine famille de polynômes. Comme les $\mathscr{H}_{q,n}$ sont des algèbres associatives, ces polynômes s'annulent pour tout q et sont donc nuls.

3. *Montrer que l'évaluation en $X = 1$ fournit un isomorphisme d'algèbres entre $\mathscr{H}_n/(X-1)$ et $\mathbb{Q}\mathfrak{S}_n$.*

   On remarque d'abord que $T_s * T_{w'}$ s'évalue en $T_{sw'}$ en $X = 1$. Par récurrence sur la longueur de w, on montre que les $\overline{T}_w$ (évalués en 1) satisfont aux relations de l'algèbre du groupe $\mathfrak{S}_n$: $\overline{T}_w \overline{T}_{w'} = \overline{T}_{ww'}$. La surjectivité est évidente, et l'injectivité provient de l'égalité des dimensions comme espaces vectoriels sur $\mathbb{Q}$.

Actions de groupes sur les représentations

F.22. Exercice (Tensorisation par une représentation de degré 1)

Soient G un groupe fini et V un espace vectoriel et soit $\rho : G \to \mathrm{GL}(V)$ une représentation. Soit ε un morphisme de G dans $\mathbb{C}^*$, c'est-à-dire une représentation de degré 1 de G. On considère le morphisme $\rho_\varepsilon : G \to \mathrm{End}(V)$, $g \mapsto \varepsilon(g)\rho(g)$.

1. *Montrer que si ρ est une représentation irréductible, alors ρ_ε est encore une représentation irréductible de G.*

   D'abord, ρ_ε est encore un morphisme. Pour l'irréductibilité, on peut par exemple vérifier que son caractère est de norme 1.

2. *En déduire une action, dite* action de tensorisation, *de* $\mathrm{Mor}(G, \mathbb{C}^*)$ *sur* $\mathrm{Irr}(G)$.

3. *Exemple : on considère la représentation standard ρ de $\mathfrak{S}_3$ (de degré 2) et sa représentation alternée ε. Montrer que ρ_ε est isomorphe à ρ.*

F.23. Exercice (Action de $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ sur $\mathrm{Irr}(G)$)

Soit G un groupe fini ; on note comme d'habitude $\mathrm{Irr}(G)$ l'ensemble de ses caractères irréductibles. Soit $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ le groupe de Galois de $\mathbb{C}$ sur $\mathbb{Q}$, i.e. *le groupe des automorphismes du corps $\mathbb{C}$ qui laissent (forcément) fixe $\mathbb{Q}$. On note $\mathrm{Aut}(G)$ le groupe des automorphismes de G et $\mathrm{Int}(G)$ le sous-groupe distingué de ses automorphismes intérieurs. Nous proposons dans cet exercice et les deux suivants des actions naturelles de groupes sur $\mathrm{Irr}(G)$.*

1. *Si γ est dans $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, on note $\phi(\gamma)$ l'application de $\mathscr{M}_n(\mathbb{C})$ dans lui-même qui envoie la matrice $A = (a_{ij})$ vers la matrice $\phi(\gamma)(A) = (g(a_{ij}))$. Montrer que ϕ définit un morphisme de $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ vers le groupe des automorphismes de la $\mathbb{Q}$-algèbre $\mathscr{M}_n(\mathbb{C})$.*

2. *Soit $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ une représentation du groupe G. Montrer que $\rho_\gamma = \phi(\gamma) \circ \rho$ définit une représentation complexe de G pour tout γ dans $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$. Montrer de plus que si ρ est irréductible, alors ρ_γ l'est également.*

   Supposer par l'absurde que la représentation ρ_γ se décompose, et montrer alors que $\rho = \phi(\gamma^{-1}) \circ \rho_\gamma$ se décompose aussi.

3. *En déduire que la formule $\gamma \cdot \chi_\rho = \chi_{\rho_\gamma}$ définit une action de $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ sur $\mathrm{Irr}(G)$.*

F.24. Exercice (Action du groupe $\mathrm{Out}(G)$ sur $\mathrm{Irr}(G)$)

Mêmes hypothèses et notations que dans l'exercice précédent.

1. *Montrer que l'on définit une action du groupe $\mathrm{Aut}(G)$ sur $\mathrm{Irr}(G)$ en posant $(g \cdot \chi)(h) = \chi(g^{-1}hg)$, pour tous g, h dans G et χ dans $\mathrm{Irr}(G)$.*

2. *Montrer que l'action restreinte à $\mathrm{Int}(G)$ est triviale et en déduire une action du groupe $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$ des automorphismes extérieurs de G sur $\mathrm{Irr}(G)$.*

3. *Décrire les orbites de ces actions lorsque G est l'un des groupes suivants : $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}^*$), $\mathfrak{S}_4$, $\mathfrak{S}_5$, $\mathfrak{A}_4$ ou $\mathfrak{A}_5$.*

F.25. Exercice (Action de $\mathrm{Mor}(G,\mathbb{C}^*)$ sur $\mathrm{Irr}(G)$)

Mêmes hypothèses et notations que dans les deux exercices précédents.

Soit $\mathrm{Mor}(G,\mathbb{C}^*)$ *l'ensemble des morphismes du groupe* G *vers le groupe multiplicatif des complexes. On munit* $\mathrm{Mor}(G,\mathbb{C}^*)$ *d'une structure de groupe par* $(\alpha\cdot\beta)(g)=\alpha(g)\beta(g)$ *pour tout* g *de* G *et tout couple* (α,β) *de morphismes de* $\mathrm{Mor}(G,\mathbb{C}^*)$.

1. *Soit* $\rho : G\to \mathrm{GL}_n(\mathbb{C})$ *une représentation de* G. *Montrer que l'application* $\alpha\otimes\rho : G\to\mathrm{GL}_n(\mathbb{C})$, $g\mapsto\alpha(g)\rho(g)$ *est également une représentation de* G.
2. *Soit* α *dans* $\mathrm{Mor}(G,\mathbb{C}^*)$ *et soit* ρ *une représentation complexe de* G. *Montrer que la formule* $\alpha\cdot\chi_\rho=\chi_{\alpha\otimes\rho}$ *définit une action du groupe* $\mathrm{Mor}(G,\mathbb{C}^*)$ *sur* $\mathrm{Irr}(G)$.
3. *Décrire les orbites de cette action lorsque* G *est l'un des groupes suivants :* $\mathbb{Z}/n\mathbb{Z}$ *(*$n\in\mathbb{N}^*$*),* $\mathfrak{S}_4$ *ou* $\mathfrak{S}_5$.

Table des caractères et applications

F.26. Exercice. *On veut montrer que l'on peut retrouver le treillis (pour l'inclusion) des sous-groupes distingués de* G *à partir de la table des caractères de* G.

1. *Montrer, pour tout caractère irréductible* χ, *que* $K_\chi=\{g,\chi(g)=\chi(e)\}$ *est le noyau de la représentation correspondante.*

   On a $\chi(g)=\mathrm{tr}\big(\rho(g)\big)$, où $\rho(g)$ a pour valeurs propres des racines de l'unité. Le cas d'égalité de l'inégalité triangulaire assure que la somme est égale au degré de la représentation si et seulement si toutes ces valeurs propres valent 1.

2. *Si* K *est un sous-groupe distingué de* G, *montrer que* K *est le noyau de la représentation régulière du groupe* G/K *(vue comme* G*-représentation par passage au quotient). En déduire que* K *est l'intersection de noyaux de* G*-modules irréductibles.*

   La régulière est fidèle, ce qui implique le premier résultat. Grâce au théorème de semi-simplicité des représentations, on voit que tout noyau de représentation est intersection de noyaux de représentations irréductibles.

3. *Déduire que le treillis engendré par les* K_i *(*$i\in\mathrm{Irr}(G)$*) est égal au treillis des sous-groupes distingués de* G.

4. *Observer ce résultat sur la table de* $\mathfrak{S}_3$ *et celle de* $\mathfrak{S}_4$.

F.27. Exercice. *Soit G un groupe fini. Montrer que l'intersection des noyaux des représentations de degré 1 de G est égale au groupe dérivé $D(G)$.*

L'inclusion inverse est claire puisque le quotient de G par le noyau d'une représentation de degré 1 s'injecte dans le groupe abélien $\mathbb{C}^*$. Pour montrer l'inclusion, il suffit de voir que la représentation régulière, voir §C.1 du groupe abélien $G/D(G)$ est fidèle et somme directe de représentations de degré 1 de $G/D(G)$. Donc, par passage au quotient, on obtient une représentation de G de noyau $D(G)$ qui se réalise ainsi en une intersection de noyaux de représentations de degré 1.

F.28. Exercice (Critère de simplicité)

En utilisant l'exercice F.26, montrer qu'un groupe est simple si et seulement si tous les K_i, pour $i \in \mathrm{Irr}(G)$ non trivial, sont réduits à l'identité. Observer la simplicité de $\mathfrak{A}_5$ sur sa table des caractères.

Pour chaque ligne de la table des caractères, à l'exception de la ligne correspondant au caractère trivial, on voit que le degré n'apparaît qu'une fois (dans la première colonne).

F.29. Exercice. *Montrer que si, sur une des lignes de la table des caractères, on a $\chi(g) = \chi(e)$ implique $g = e$, alors le centre de G est cyclique.*

En effet, d'après l'exercice F.26, cela implique que la représentation irréductible S_i correspondante est fidèle. Par le lemme de Schur, le centre de G s'injecte dans le groupe $\mathbb{C}^*$. Or, tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

F.30. Exercice

1. *Si le caractère χ est à valeurs dans $\mathbb{R}$, est-ce que les représentations correspondantes V_χ et V_χ^* sont isomorphes ?*

   Oui, et réciproquement ! C'est dû au fait que le caractère caractérise.

2. *Est-ce que dans ce cas il existe une représentation réelle qui réalise χ ?*

   Non ! on le voit avec le groupe quaternionique H_8 par le théorème E.6, voir aussi l'exercice F.32.

F.31. Exercice. *Montrer que si un caractère a ses valeurs dans $\mathbb{Q}$, alors ses valeurs sont dans $\mathbb{Z}$.*

On a vu que le caractère d'un élément g de G est toujours un entier algébrique, puisqu'il est somme de racines de l'unité. Or, tout entier algébrique rationnel est entier.

F.32. Exercice (Représentation quaternionique)

Nous voulons justifier l'appellation représentation quaternionique *dans le cadre de la définition E.9. On suppose donc que V est un G-module irréductible muni d'une forme alternée ω non dégénérée G-invariante. On munit V d'une forme hermitienne G-invariante $\langle \cdot, \cdot \rangle$.*

1. *Montrer qu'il existe une application semi-linéaire non nulle ψ de V dans lui-même tel que $\langle \psi(u), v \rangle = \omega(u, v)$ pour tout u, v de V. Montrer alors que ψ^2 est un morphisme de représentations (linéaire) tel que $\langle \psi^2(u), v \rangle = -\langle \psi(v), \psi(u) \rangle$.*

   Ce n'est rien d'autre que la preuve de la proposition E.5 en remplaçant β par ω et ϕ par ψ.

2. *Montrer que ψ^2 est une homothétie, dont le rapport $-\lambda$ est un réel négatif. Quitte à remplacer l'application ψ par $\psi/\sqrt{\lambda}$, on pourra supposer que l'on a : $\psi^2 = -\mathrm{Id}_V$.*

3. *Montrer que le G-module V peut être muni d'une structure de $\mathbb{H}$-module,* i.e. *qu'il existe un morphisme d'algèbre $\mathbb{H} \to \mathrm{End}(V)$ non trivial, et qui commute à l'action de G,* i.e. *$h \cdot \big(\rho(g)(v)\big) = \rho(g)(h \cdot v)$ pour $h \in \mathbb{H}$, $g \in G$ et $v \in V$.*

   On connaît les relations satisfaites par les générateurs classiques i, j et k de $\mathbb{H}$. On pourra envoyer i sur la multiplication μ_i de V (on rappelle que V est un espace complexe !), j sur ψ (qui est semi-linéaire), et k sur $\mu_i \psi$. Par construction, ces morphismes commutent à l'action de G.

Arithmétique et représentations

F.33. Exercice (Le degré d'une représentation irréductible divise l'ordre). *Voici une incursion intéressante de l'arithmétique dans la théorie des représentations, qui demande quelques connaissances élémentaires sur les $\mathbb{Z}$-modules. Soit G un groupe fini et soit χ un caractère irréductible de G.*

1. *Montrer que pour tout g dans G, $\chi(g)$ est un entier algébrique.*

   La trace $\chi(g)$ est une somme de valeurs propres, donc une somme de racines de l'unité, par Lagrange. Et une somme d'entiers algébriques est encore un entier algébrique.

2. *Soit C_j une classe de conjugaison de G. Montrer que $z_j = \sum_{g \in C_j} g$ est dans le centre de $\mathbb{Z}[G]$, et que ce centre est un $\mathbb{Z}$-module de type fini.*

   Le centre est engendré comme $\mathbb{Z}$-module par les z_j, pour tout j.

3. *Soit V_i une représentation irréductible. Montrer que z_j agit sur V_i par une homothétie de rapport λ_{ij} telle que $\lambda_{ij} \dim V_i = |C_j| \chi_i(C_j)$.*

   Par le lemme de Schur, comme z_j est central, il agit comme un scalaire sur V_i. La formule de la trace est directe.

4. *Montrer que les λ_{ij} sont des entiers algébriques.*
   Les z_j sont algébriques sur $\mathbb{Z} = \mathbb{Z}e$, d'après ce qui précède. Si ρ est le morphisme de représentations, alors, en prenant l'image par ρ, on obtient le résultat.
5. *Montrer que l'on a :* $\dfrac{|G|}{\dim V_i} = \sum_j \lambda_{ij}\overline{\chi_i(C_j)}$.
   La formule d'orthogonalité donne : $\sum_j |C_j|\overline{\chi_i(C_j)}\chi_i(C_j) = |G|$.
6. *En déduire que le degré d'une représentation irréductible divise l'ordre du groupe.*
   Comme $|G|/\dim V_i$ est un entier algébrique rationnel, c'est un entier tout court.

F.34. Exercice. *Montrer que si le degré d'une représentation irréductible est strictement supérieur à 1, et que le caractère χ est à valeurs dans $\mathbb{Z}$, alors le caractère s'annule sur au moins une classe de conjugaison.*

Cela vient de ce que les caractères ont pour norme 1, c'est-à-dire : $|G| = \sum_{g\in G} |\chi(g)|^2$, avec $\chi(e) = \dim V_\chi$.

F.35. Exercice (Zéros sur les lignes des tables de caractères)

Nous allons montrer que, dans l'exercice F.34, on peut se passer de l'hypothèse entière du caractère. Soit une représentation irréductible de caractère χ telle que pour tout g, les $\chi(g)$ sont non nuls. Nous allons montrer que le degré de la représentation est alors égal à 1.

1. *En faisant agir le groupe de Galois* $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ *sur le caractère χ comme dans F.23, montrer que l'on obtient une famille finie de caractères χ_i ($1 \leqslant i \leqslant k$) tels que $\prod_i \chi_i(g)$ est entier non nul, et donc $\geqslant 1$.*
   Comme χ est à valeurs dans un ensemble fini d'entiers algébriques, il est à valeurs dans un corps $\mathbb{K}$ de degré fini de $\mathbb{Q}$. On obtient bien un nombre fini de caractères, puisque $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})\cdot\chi = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})\cdot\chi$ est fini. L'autre assertion est claire par définition de l'action.
2. *Montrer l'inégalité* $\sum_i |\chi_i(g)|^2 \geqslant k$.
   Comme la moyenne arithmétique est plus grande que la moyenne géométrique, on obtient l'inégalité voulue.
3. *Montrer que l'on a* $k|G| = \sum_i \sum_g |\chi_i(g)|^2 \geqslant k|G|$, *et en déduire que l'inégalité de 2 est une égalité pour tout g.*
4. *Conclure.*
   Si d est le degré de la représentation, on a : $kd^2 = \sum_i |\chi_i(e)|^2 = k$.

On peut exprimer le résultat précédent sous la forme complètement élémentaire suivante, peut-être plus surprenante : si un sous-groupe fini G du groupe linéaire $\mathrm{GL}_n(\mathbb{C})$, avec $n > 1$, ne laisse stable aucun sous-espace non trivial de $\mathbb{C}^n$, alors G contient une matrice de trace nulle.

F.36. Exercice (Un zéro sur chaque ligne, variante)

Voici une légère variante de l'exercice F.35, qui n'utilise pas l'action du groupe de Galois sur les caractères. On note pour cela que si le groupe G est d'ordre n, alors les caractères sont dans le corps $\mathbb{Q}[\omega]$ engendré par une racine primitive ω de l'unité. On note aussi que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ agit par automorphismes sur le corps $\mathbb{Q}[\omega]$ par $\varphi_m(\omega) = \omega^m$.

1. *Soit χ un caractère ; on pose $N(\chi) = \prod_{g\in G} |\chi(g)|^2$. Montrer que $N(\chi)$ appartient à $\mathbb{Q}[\omega]$, puis que $\varphi_m\big(\chi(g)\big) = \chi(g^m)$.*

   On a : $|\chi(g)|^2 = \chi(g)\chi(g^{-1})$. Par suite, comme $\chi(g) \in \mathbb{Q}[\omega]$ pour tout g, on a : $N(\chi) \in \mathbb{Q}[\omega]$. Maintenant, si l'on note ω_i les valeurs propres de g (ce sont des racines n-ièmes de l'unité), on a : $\varphi_m\big(\chi(g)\big) = \varphi_m(\sum_i \omega_i) = \sum_i \omega_i^m = \chi(g^m)$.

2. *En déduire que $N(\chi)$ appartient à $\mathbb{Z}$.*

   On déduit de la question précédente que $N(\chi)$ est invariant par le groupe de Galois de $\mathbb{Q}[\omega]$ sur $\mathbb{Q}$ et, ainsi, $N(\chi) \in \mathbb{Q}$. Comme il est entier sur $\mathbb{Z}$, il est dans $\mathbb{Z}$.

3. *Conclure.*

   Par l'absurde : s'il n'y avait pas d'élément de trace nulle, on aurait : $N(\chi) \geqslant 1$. On conclut comme dans l'exercice F.35 à l'aide de la comparaison entre moyenne géométrique et moyenne arithmétique.

Action de groupe sur une algèbre de polynômes, série de Molien

F.37. Exercice (Préliminaire : série génératrice d'un espace gradué). *Un* espace vectoriel gradué *(sur $\mathbb{N}$) sur un corps donné est un espace vectoriel R muni d'une décomposition : $R = \bigoplus_{n\in\mathbb{N}} R_n$, où chaque R_n est un sous-espace vectoriel de dimension finie. On définit la* série génératrice (des dimensions) *de R comme la série formelle : $f_R(t) = \sum_{n\geqslant 0} \dim(R_n) t^n \in \mathbb{Z}[[t]]$.*

Si, de plus, R est muni d'une structure d'algèbre, on dit que c'est une algèbre graduée *si l'on a pour tous m et n entiers l'inclusion : $R_m R_n \subset R_{m+n}$.*

1. *Fixons un entier naturel d. Vérifier que l'algèbre des polynômes $R = \mathbb{C}[x]$ est graduée en prenant : $R_{dk} = \mathbb{C}x^k$ pour tout k dans $\mathbb{N}$ et $R_n = 0$ si n n'est pas un multiple de d (cela revient à donner le degré d à x) et que la série génératrice correspondante est $1/(1-t^d)$.*

2. *Soient r et $d_1, \dots, d_r$ des entiers naturels non nuls. On note R l'algèbre des polynômes en r indéterminées $x_1, \dots, x_r$. Pour n entier naturel, on note R_n le sous-espace vectoriel engendré par les monômes $x_1^{k_1} \cdots x_r^{k_r}$ pour lesquels $k_1 d_1 + \cdots + k_r d_r = n$. Cela revient à dire que l'on donne à x_i le degré d_i.*

   Vérifier que R est une algèbre graduée et que l'on a :

$$f_R(t) = \prod_{i=1}^{r} \frac{1}{1 - t^{d_i}}.$$

   La première partie est claire. Pour f_R, constater que la dimension de R_n est le nombre de monômes de la forme indiquée. Or, on obtient chaque monôme exactement une fois en facteur de t^n dans la série formelle

$$\prod_{i=1}^{r} \frac{1}{1 - x_i t^{d_i}} = \prod_{i=1}^{r} \sum_{k_i \geqslant 0} x_i^{k_i} t^{k_i d_i},$$

   de sorte que le coefficient cherché s'obtient en remplaçant chaque x_i par 1 dans cette série formelle en t à coefficients dans $\mathbb{Z}[x_1, \dots, x_r]$.

3. *Un* sous-espace vectoriel gradué *d'un espace gradué $R = \bigoplus_{n \geqslant 0} R_n$ est un sous-espace vectoriel T tel que : $T = \bigoplus_{n \geqslant 0} (T \cap R_n)$ pour tout n. Vérifier que R/T est naturellement muni d'une structure d'espace gradué et que l'on a : $f_R(t) = f_T(t) + f_{R/T}(t)$.*

4. *On suppose que R est une algèbre graduée intègre et que a est un élément homogène de degré d de R. Montrer que l'idéal $T = aR$ est un espace gradué, que le quotient R/T est une algèbre graduée et que l'on a l'égalité suivante entre séries génératrices : $f_{R/aR}(t) = (1 - t^d) f_R(t)$.*

   L'hypothèse d'intégrité garantit que l'application $\mu_a : R \to R$, $x \mapsto ax$ est une injection de R_n dans R_{n+d} —et donc une bijection de R_n sur T_{n+d} – pour tout n.

F.38. Exercice (Prolongement d'une représentation sur l'algèbre des polynômes et caractères)

Soit $\phi : G \to \mathrm{GL}(E)$ une représentation du groupe fini G sur un espace vectoriel E de dimension n. On plonge l'espace E dans l'algèbre de polynômes en E notée $\mathscr{S}(E)$, voir VIII-A.4.

1. *Montrer que l'action de G se prolonge de façon unique en une action par automorphismes sur $\mathscr{S}(E)$, qui stabilise le sous-espace homogène de degré d, noté $\mathscr{S}(E)_d$, de l'algèbre de polynômes $\mathscr{S}(E)$. On notera dans la suite ϕ_d la représentation de G sur l'espace $\mathscr{S}(E)_d$ ainsi définie.*

   Il s'agit tout simplement du corollaire VIII-A.5.

2. *Soit g dans G et soient $\lambda_1, \dots, \lambda_n$ les valeurs propres de $\phi(g)$. Montrer que les valeurs propres de $\phi_d(g)$ sont les produits $\prod \lambda_i^{d_i}$, où $(d_i)_{1 \leqslant i \leqslant n}$ parcourt les multi-indices tels que $\sum_{i=1}^n d_i = d$.*
   On prend pour base de E une base x_i de vecteurs propres. Par la formule du corollaire VIII-A.5, les monômes $\prod_{i=1}^n x_i^{d_i}$, avec $\sum_{i=1}^n d_i = d$, constituent une base de vecteurs propres de $\mathscr{S}(E)_d$.
3. *En déduire que le caractère χ_d de la représentation ϕ_d est donné par $\chi_d(g) = \sum \prod_{i=1}^n \lambda_i^{d_i}$, où la somme porte sur les multi-indices tels que $\sum_{i=1}^n d_i = d$.*

F.39. Exercice. *On reprend les notations de l'exercice F.38, avec E un espace sur le corps des complexes. On veut montrer la formule suivante (comparer à la proposition XI-A.8) :*

$$\frac{1}{\det\bigl(\mathrm{Id} - t\phi(g)\bigr)} = \sum_{d \in \mathbb{N}} \chi_d(g) t^d,$$

pour tout t complexe de module strictement inférieur à 1 ou[22] *comme égalité de séries formelles.*

1. *Les $\lambda_1, \dots, \lambda_n$ étant les valeurs propres de $\phi(g)$, montrer que*

$$\frac{1}{\det\bigl(\mathrm{Id} - t\phi(g)\bigr)} = 1 \Big/ \prod_{i=1}^n (1 - \lambda_i t).$$

   Le polynôme caractéristique s'écrit : $\det\bigl(x\,\mathrm{Id} - \phi(g)\bigr) = \prod_i (x - \lambda_i)$. On pourra supposer t non nul pour partir du bon pied.

2. *Montrer que* $\displaystyle \frac{1}{\det\bigl(\mathrm{Id} - t\phi(g)\bigr)} = \sum_{d \in \mathbb{N}} \sum_{\substack{(d_i) \in \mathbb{N}^n \\ \sum_i d_i = d}} \Bigl(\prod_i \lambda_i^{d_i}\Bigr) t^d.$

   Il suffit de développer la série géométrique $(1 - \lambda_i t)^{-1} = \sum_{d_i \in \mathbb{N}} \lambda_i^{d_i} t^{d_i}$, puis de faire le produit de Cauchy des séries obtenues.
3. *Déduire la formule désirée à l'aide de l'exercice F.38.*
4. *Montrer que $|\chi_d(g)| \leqslant \dim \mathscr{S}(E)_d$. En déduire que le rayon de convergence*[23] *de la série en t est supérieur à 1.*
   Comme G est fini, les λ_i sont des racines de l'unité, par Lagrange, et donc la trace de $\phi_d(g)$ est de module inférieur à la dimension de l'espace sur lequel il agit. On connaît le degré de l'espace des polynômes homogènes de degré d à n variables (ou on peut le voir par récurrence) : $\dim \mathscr{S}(E)_d = \binom{n+d-1}{d}$. Cela donne l'assertion sur le rayon de convergence.

[22] C'est mieux, parce que c'est moins cher !
[23] Tiens ! Drôle d'idée de faire converger des séries qui pourraient rester formelles !

F.40. Exercice (Série de Molien, formule de Molien classique)

Comme dans l'exercice F.38, soit une représentation $\phi : G \to \mathrm{GL}(E)$ du groupe fini G sur un espace vectoriel E de dimension n. L'action de G se prolonge en une action par automorphismes sur $\mathscr{S}(E)$ et l'on veut calculer la sous-algèbre des invariants $\mathscr{S}(E)^G$ sous l'action de G (on vérifie que c'est bien une sous-algèbre).

1. *Soient $\mathscr{S}(E)_d$ comme dans l'exercice F.38 et $\mathscr{S}(E)_d^G$ le sous-espace des invariants de $\mathscr{S}(E)_d$ sous l'action de G. Montrer que $\mathscr{S}(E)^G = \bigoplus_{d\in\mathbb{N}} \mathscr{S}(E)_d^G$.*

   L'inclusion inverse est claire. Pour l'inclusion directe, il suffit de décomposer un élément de $\mathscr{S}(E)^G$ dans $\bigoplus_{d\in\mathbb{N}} \mathscr{S}(E)_d$ et de voir que comme G stabilise chaque composante homogène, la décomposition se fait dans $\bigoplus_{d\in\mathbb{N}} \mathscr{S}(E)_d^G$.

2. *Montrer la relation : $\dim \mathscr{S}_d^G = \dfrac{1}{|G|} \displaystyle\sum_{g\in G} \chi_d(g)$.*

   Par la proposition A.21, $|G|^{-1} \sum_{g\in G} \chi_d(g)$ est la trace de la projection de $\mathscr{S}_d$ sur $\mathscr{S}_d^G$. C'est donc bien $\dim \mathscr{S}_d^G$.

3. *Pour $t \in \mathbb{C}$, on pose : $S(t) = \sum_{d\in\mathbb{N}} \dim \mathscr{S}(E)_d^G t^d$, appelée série de Molien pour l'action de G sur $\mathscr{S}(E)$. Montrer l'égalité :*

$$S(t) = \frac{1}{|G|} \sum_{g\in G} \frac{1}{\det\bigl(\mathrm{Id} - t\phi(g)\bigr)}.$$

   C'est la question précédente conjointe à l'exercice F.39.

Les trois exercices suivants calculent et interprètent la série de Molien pour le groupe à deux éléments... Étonnamment, ce n'est pas tout à fait trivial !

F.41. Exercice (Un cas d'école). *Soit $E = \mathbb{C}$; on note x une base de E, de sorte que l'algèbre symétrique $\mathscr{S}(E)$ s'identifie aux polynômes $\mathbb{C}[X]$. On fait agir le groupe $G = \{-1, 1\}$ par multiplication par un signe ± 1 sur x. Vérifier que l'algèbre des invariants est $\mathbb{C}[x^2]$, que sa série de Poincaré est $1/(1-t^2)$ et que la formule de Molien est satisfaite. Étendre le résultat aux groupe des racines n-ièmes de l'unité pour tout entier $n \geqslant 2$.*

F.42. Exercice (Un quotient lisse). *Soit $E = \mathbb{C}^2$; on note (x_1, x_2) une base de E et l'on fait agir le groupe symétrique $G = \mathfrak{S}_2 = \{e, \sigma\}$ par permutation des coordonnées : $\sigma(x_1) = x_2$, $\sigma(x_2) = x_1$. Il est bien connu que tout polynôme invariant s'écrit de façon unique comme polynôme en les polynômes symétriques élémentaires $e_1 = x_1 + x_2$ et $e_2 = x_1 x_2$. On va retrouver cela.*

1. *Montrer que la série de Molien est* $S(t) = \dfrac{1}{(1-t)(1-t^2)}$.

   La formule générale donne : $S(t) = \dfrac{1}{2}\Big(\dfrac{1}{(1-t)^2} + \dfrac{1}{(1-t^2)}\Big)$.

2. *Montrer que* e_1 *et* e_2 *engendrent* $\mathscr{S}(E)^G$.

   Dans un polynôme symétrique général, si un monôme $x_1^a x_2^b$ apparaît, alors $x_1^b x_2^a$ a le même coefficient ; il suffit donc de montrer que leur somme est engendrée par e_1 et e_2 : c'est $e_2^m(x_1^k + x_2^k)$, avec $m = \min(a,b)$ et $k = \max(a,b) - m$. On exprime alors $x_1^k + x_2^k$ en fonction de e_1 et e_2, ce qui se fait facilement par récurrence sur k.

3. *On se place dans l'algèbre de polynômes* $\mathbb{C}[e_1, e_2]$, *dont on fait une algèbre graduée, comme dans l'exercice F.37, en prenant* e_1 *de degré* 1 *et* e_2 *de degré* 2. *Vérifier que le morphisme d'algèbres* $\mathbb{C}[e_1,e_2] \to \mathscr{S}(E)^{\mathfrak{S}_2}$, $e_1 \mapsto x_1 + x_2$, $e_2 \mapsto x_1 x_2$ *envoie polynômes homogènes de degré donné (au sens précédent) sur des polynômes de même degré (au sens usuel) en* x_1 *et* x_2.

4. *Montrer que c'est un isomorphisme :* $\mathbb{C}[e_1,e_2] \simeq \mathscr{S}(E)^{\mathfrak{S}_2}$.

   La surjectivité vient de la première question. L'injectivité vient du calcul des dimensions degré par degré, car les séries génératrices des deux algèbres graduées sont : $1/(1-t)(1-t^2)$ (comparer le résultat de l'exercice F.37 et la série de Molien).

Le résultat s'interprète en disant que le quotient $\mathbb{C}^2/\mathfrak{S}_2$ *est isomorphe (comme variété algébrique) à* $\mathbb{C}^2$. *On a avec l'exercice précédent les illustration les plus simples d'un fameux* théorème de Chevalley *: étant donné un sous-groupe fini* G *de* $\mathrm{GL}_d(\mathbb{C})$, *le quotient* $\mathbb{C}^d/G$ *est isomorphe à* $\mathbb{C}^d$ *(comme variété algébrique) si et seulement s'il est lisse (comme variété algébrique), ou encore si* G *est engendré par des* pseudo-réflexions, i.e. *par des éléments* g *tels que* $\operatorname{codim}\ker(g - \mathrm{Id}) = 1$.

F.43. Exercice (Un quotient singulier)

On reprend $E = \mathbb{C}^2$ *et sa base* (x_1, x_2). *On considère l'action du groupe cyclique* $G = \mathbb{Z}/2\mathbb{Z} = \{-\mathrm{Id}, \mathrm{Id}\}$ *sur* E.

1. *Vérifier que la série de Molien est* $S(t) = \dfrac{1+t^2}{(1-t^2)^2}$.

   Il suffit de montrer que l'on a $S(t) = \dfrac{1}{2}\Big(\dfrac{1}{(1-t)^2} + \dfrac{1}{(1+t)^2}\Big)$.

2. *On va retrouver ce résultat grâce à la structure de* $\mathscr{S}(E)^G$. *On identifie* $\mathscr{S}(E)$ *et* $\mathbb{C}[x_1,x_2]$. *L'action de* $\sigma = -\mathrm{Id}$ *sur un monôme est donnée par :* $\sigma \cdot x_1^{a_1} x_2^{a_2} = (-1)^{a_1+a_2} x_1^{a_1} x_2^{a_2}$ *(*a_1, a_2 *entiers) par la formule du corollaire VIII-A.5.*

Vérifier que l'on a la décomposition $\mathscr{S}(E)^G = \mathbb{C}[x_1^2, x_2^2] \oplus \mathbb{C}[x_1^2, x_2^2]x_1x_2$. *En déduire un nouveau calcul de la série de Molien.*

Cela signifie que $\mathscr{S}(E)^G$ est un $\mathbb{C}[x_1^2, x_2^2]$-module libre de rang 2.

3. *Vérifier que l'on a aussi :* $S(t) = (1-t^4)/(1-t^2)^3$.

4. *On gradue l'algèbre des polynômes en trois variables* $R = \mathbb{C}[u, v, w]$ *en donnant le degré 2 aux indéterminées* u, v *et* w. *On note* $a = uv - w^2$. *Soit* $\pi : \mathbb{C}[u, v, w] \to \mathscr{S}(E)^G$ *l'unique morphisme d'algèbres tel que :* $\pi(u) = x_1^2$, $\pi(v) = x_2^2$, $\pi(w) = x_1x_2$. *Vérifier que* π *induit un morphisme surjectif qui préserve le degré* $\bar{\pi} : R/aR \to \mathscr{S}(E)^G$. *Montrer que* $\bar{\pi}$ *est un isomorphisme.*

Par l'exercice F.37, l'algèbre R/aR est graduée et sa série génératrice est $(1-t^4)/(1-t^2)^3$, ce qui donne l'injectivité degré par degré.

On a donc prouvé l'isomorphisme :

$$\mathbb{C}[x_1, x_2]^{\{\pm \mathrm{Id}\}} \simeq \mathbb{C}[u, v, w]/(uv - w^2).$$

Le membre de droite est naturellement l'algèbre des fonctions sur le cône isotrope (singulier !) de la forme quadratique $uv - w^2$. *C'est une utilisation typique de la formule de Molien pour établir que l'on a bien toutes les relations entre des générateurs de l'algèbre des invariants. Voir la figure XI-8.1 p. 529.*

F.44. Exercice (Singularités de type A)

Reprendre l'exercice F.43 pour G *égal au groupe* μ_n *des racines* n*-ièmes de l'unité pour* n *entier naturel non nul fixé, où un élément* ζ *de* μ_n *agit sur* $\mathbb{C}^2$ *comme la matrice diagonale* $\mathrm{diag}(\zeta, \zeta^{-1})$, *de déterminant* 1. *Montrer que l'on a :*

$$\mathbb{C}[x_1, x_2]^{\mu_n} = \mathbb{C}[x_1^n, x_2^n, x_1x_2] \simeq \mathbb{C}[u, v, w]/(uv - w^n).$$

F.45. Exercice (Molien plus bifluoré)

On reprend le contexte et les notations des séries de Molien. Soit S *une représentation irréductible du groupe* G, *de caractère* χ. *On considère pour tout* $d \in \mathbb{N}$ *la composante isotypique* $\mathscr{S}_{d,\chi}$ *pour le caractère* χ *de* $\mathrm{Irr}(G)$ *dans* $\mathscr{S}_d$. *On veut calculer la série de Molien généralisée :*

$$S_\chi(t) = \sum_{d \in \mathbb{N}} \dim \mathscr{S}(E)_{d,\chi} t^d.$$

On remarquera que si $\chi = \chi_0$ *est le caractère trivial, on a* $S_\chi(t) = S(t)$.

Montrer la formule de Molien :

$$S_\chi(t) = \frac{\dim S}{|G|} \sum_{g\in G} \frac{\overline{\chi(g)}}{\det\bigl(\mathrm{Id} - t\phi(g)\bigr)}.$$

Procéder comme pour la formule de Molien classique avec le corollaire B.12.

Un zeste de représentations modulaires

F.46. Exercice. *Soit p un nombre premier et soit $G = \mathbb{Z}/p\mathbb{Z}$. Montrer que la représentation sur $V = \mathbb{F}_p^2$ induite par*

$$G \longrightarrow \mathrm{GL}_2(\mathbb{F}_p), \quad g \longmapsto \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}$$

possède une sous-représentation simple S, que V/S est simple mais que V n'est pas isomorphe à la somme directe $S \oplus V/S$.

F.47. Exercice. *On suppose que $\mathbb{K} = \mathbb{F}_p$, où p est premier et l'on prend : $G = \mathrm{SL}_2(\mathbb{F}_p)$. Soit $A = \mathbb{F}_p[x,y]$ l'algèbre des polynômes en deux variables x et y. On fait agir G sur l'espace A par :*

$$\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p),\ \forall f \in A, \quad g \cdot f(x,y) = f(ax+cy, bx+dy).$$

1. *Vérifier que pour tout entier n, l'espace A_n des polynômes homogènes de degré n est une représentation de G. Quelle est sa dimension ?*
2. *Vérifier que x^p et y^p engendrent une sous-représentation de A_p irréductible isomorphe à A_1.*
3. *Soit u la matrice unipotente $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Calculer $u \cdot f_k$, où $k \in \{0,\dots,p\}$ et $f_k(x,y) = x^k y^{p-k}$.*
4. *Montrer que le quotient $A_p/(\mathbb{F}_p x^p + \mathbb{F}_p y^p)$ est irréductible et que si $p \neq 3$, il n'est pas isomorphe à A_1.*
   On fait une récurrence en utilisant u : on montre que si M est une sous-représentation non nulle, alors elle contient $x^{p-1}y$. Puis, on montre en utilisant ${}^t u$ que si M contient $x^{p-1}y$, il contient tout le quotient $A_p/(\mathbb{F}_p x^p + \mathbb{F}_p y^p)$. Pour la dernière assertion, utiliser la dimension !
5. *Montrer que si $p \neq 3$, l'algèbre des endomorphismes de A_p est isomorphe à $\mathbb{F}_p$ (alors que A_p n'est pas irréductible). En particulier, A_p n'est pas isomorphe à la somme directe de $\mathbb{F}_p x^p + \mathbb{F}_p y^p$ et de $A_p/(\mathbb{F}_p x^p + \mathbb{F}_p y^p)$.*
   En utilisant l'action du sous-groupe (cyclique) des matrices diagonales sur les vecteurs f_k, montrer qu'un endomorphisme de A_p est diagonalisable et que tous les f_k ont la même valeur propre. On pourra montrer que si $p = 3$, l'algèbre des endomorphismes est isomorphe à l'algèbre des nombres duaux $\mathbb{F}_3[X]/(X^2)$.

6. *On prend à présent $n = 2p - 2$. Montrer que le sous-espace engendré par les f_k ($0 \leqslant k \leqslant 2p-2$ et $k \neq p-1$) est stable par G et que le quotient est isomorphe à la représentation triviale.*

   C'est un cas particulier du résultat de [52].

F.48. Exercice (Des représentations de $\mathfrak{A}_5$ en caractéristique positive). *Soit $\mathbb{F}_q$ un corps fini de cardinal q. On suppose que q et impair et que $\mathbb{F}_q$ contient une racine carrée α de 5 (par exemple, $q = 9$).*

1. *Vérifier que les hypothèses sont satisfaites si q est un nombre premier congru à 1 modulo 4 ou si c'est un carré d'un nombre premier impair. Montrer qu'il existe un morphisme σ de l'anneau $R = \mathbb{Z}\big[1/2, \sqrt{5}\big]$ vers $\mathbb{F}_q$.*

   L'existence d'une racine de 5 résulte par exemple de la loi de réciprocité quadratique.

2. *Justifier l'existence d'un morphisme $\mathfrak{A}_5 \to \mathrm{GL}_3(R)$ et en déduire l'existence d'une représentation $\mathfrak{A}_5 \to \mathrm{SO}_3(\mathbb{F}_q)$.*

   On part de la représentation irréductible $\rho : \mathfrak{A}_5 \to \mathrm{GL}_3(\mathbb{R})$. Or, les matrices des générateurs $\rho\big((12)(34)\big)$ et $\rho\big((12345)\big)$ dans une base idoine, que l'on a calculées p. 442, sont à coefficients dans R : cela s'étend à tous les éléments du groupe : $\rho(\mathfrak{A}_5) \subset \mathrm{GL}_3(R)$. Ensuite, le morphisme σ induit un morphisme noté encore $\sigma : \mathrm{GL}_3(R) \to \mathrm{GL}_3(\mathbb{F}_q)$. Une égalité ${}^tAA = \mathrm{I}_3$ dans $\mathrm{GL}_3(R)$ reste satisfaite par $\sigma(A)$ dans $\mathrm{GL}_3(\mathbb{F}_q)$, si bien que l'on tombe dans $\mathrm{O}_3(\mathbb{F}_q)$, et même dans $\mathrm{SO}_3(\mathbb{F}_q)$ par simplicité de $\mathfrak{A}_5$.

3. *Soit $\phi = 2^{-1}(1+\alpha)$. Justifier que « l'icosaèdre »*

$$\bar{P} = \{(\pm\phi, \pm 1, 0), (0, \pm\phi, \pm 1), (\pm 1, 0, \pm\phi)\},$$

   inclus dans $\mathbb{F}_q^3$, est stable par l'image de $\mathfrak{A}_5$.

   Les mêmes formules définissent un icosaèdre P dans $R^3 \subset \mathbb{R}^3$ qui est préservé par $\rho(\mathfrak{A}_5)$ et, en un sens évident, on a : $\bar{P} = \sigma(P)$. Une égalité $Av = v'$, où $A \in \mathrm{GL}_3(R)$ et $v, v' \in R^3$, implique $\sigma(A)\sigma(v) = \sigma(v')$.

4. *Montrer que cette représentation est irréductible.*

   Si elle ne l'était pas, elle admettrait une droite ou un plan stable (dimension trois !). Comme les matrices sont orthogonales, il y aurait une droite stable, vecteur propre commun à tous les éléments du groupe. Or, pour un élément g d'ordre 2 ou 5, les valeurs propres de $\rho(g)$ appartiennent à R (vérifier !) : une droite stable dans pour un tel g est donc l'image d'un vecteur propre. D'après les matrices de la p. 442, c'est impossible : les seuls vecteurs propres communs à (12)(34), (13)(24) et (14)(23) sont les vecteurs de la base (pourquoi ?), qui ne sont pas propres pour (12345).

F.49. Exercice (Analyse harmonique sur un cube)

Voici un ravissant toy model *de l'application de la théorie des représentations à la physique lorsque l'on travaille sur un système possédant une certaine symétrie. Il est inspiré du livre [45] d'Alexandre A. Kirillov, l'homme qui chante avec les cubes.*

On place des nombres $x_1, \dots, x_6$ sur les six faces d'un cube. Tous les jours, on remplace sur chaque face F le nombre inscrit par la moyenne arithmétique des nombres inscrits sur les quatre faces adjacentes à la face F. Quels nombres seront inscrits au n-ième jour ?

Soit V le $\mathbb{C}$-espace des fonctions de l'ensemble des faces dans $\mathbb{C}$ et soit f la fonction de V qui envoie la face F_i sur x_i. Comme le groupe $G = \mathfrak{S}_4$ agit sur le cube, et donc sur ses faces, on récupère une G-action linéaire par $(g \cdot f)(F) = f\big(g^{-1}(F)\big)$ (pour $f \in V$, $g \in G$). Si l'on identifie isométries et permutations comme dans [H2G2, proposition XII-3.15], on peut voir que le nombre de faces fixées par l'identité, une transposition, un 3-cycle, un 4-cycle, un produit de deux transpositions, est respectivement égal à 6, 0, 0, 2, 2. On voit alors, par la table des caractères de $\mathfrak{S}_4$ XI-6.2, que la représentation V se décompose en trois sous-représentations irréductibles $V = V_0 \oplus V_{\varepsilon\chi} \oplus V_\phi$, correspondant respectivement aux caractères χ_0, $\varepsilon\chi$, ϕ de la table. On voit aussi que V_ϕ correspond aux fonctions impaires sur le cube (deux faces opposées ont des valeurs opposées), et son orthogonal $V_0 \oplus V_{\varepsilon\chi}$ aux fonctions paires (deux faces opposées ont même valeur). Pour être plus précis, V_0 correspond aux fonctions constantes sur les faces, et $V_{\varepsilon\chi}$ aux fonctions paires à somme nulle. Comme l'action de G sur le cube préserve l'adjacence (genre !), il vient que la transformation faite chaque jour se traduit en un morphisme φ de G-représentations de V dans lui-même. Par le lemme de Schur (et le fait que chaque irréductible est de multiplicité 1), φ est une homothétie sur chaque composante irréductible. On voit facilement que le rapport est 1 sur V_0, $-1/2$ sur $V_{\varepsilon\chi}$ et 0 sur V_ϕ. Conclusion, le n-ième jour, la fonction sera donnée par

$$\phi^{n-1}(f) = \pi_0(f) + \big(-\tfrac{1}{2}\big)^{n-1} \pi_{\varepsilon\chi}(f),$$

où π_0 et $\pi_{\varepsilon\chi}$ sont les projecteurs sur les composantes isotypiques que l'on peut trouver au corollaire B.12. Pour être plus précis, $\pi_0(f)$ (la limite, donc) est la fonction constante égale à la moyenne μ des x_i et $\pi_0(f) + \pi_{\varepsilon\chi}(f)$ est la « partie paire » de f qui envoie à une face la moyenne des valeurs de cette face et de son opposée. On fait finalement ce que l'on pourrait appeler de l'analyse harmonique sur le cube. Les « harmoniques » sont les représentations irréductibles, et le « spectre » est ici l'ensemble des valeurs propres ou, si l'on préfère, celui des rapports d'homothétie.

Truth is singular.
Tom Tykwer, Andy Wachowski, Lana Wachowski, *Cloud atlas*, 2012.

Chapitre XI

Correspondance de McKay : caractères des sous-groupes finis de $\mathbf{SU_2(\mathbb{C})}$

Dans cette partie, on associe à chaque sous-groupe fini de $\mathrm{SU}_2(\mathbb{C})$ un graphe grâce à la théorie des caractères. *Spoiler* et stupéfaction ! Les graphes qui apparaissent de cette manière sont, à nouveau, les diagrammes de Dynkin apparus dans le théorème de Gabriel (théorème III-7.7 et définition III-B.1). Ces objets sont ubiquitaires en mathématiques : groupes de Lie, formes quadratiques, groupes engendrés par des réflexions, représentations des carquois, théorie des singularités, autant de théories où ils interviennent de façon cruciale. Cette correspondance entre les sous-groupes de $\mathrm{SU}_2(\mathbb{C})$ et ces graphes a été mise en évidence par McKay dans les deux articles très courts [53] et [54], dont on détaille les calculs : ce qui semblait au départ une coïncidence numérique a été la source de travaux ultérieurs très profonds et très étonnants mêlant géométrie algébrique et théorie des représentations.

Plus précisément, grâce à l'étude des sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$ et au morphisme exceptionnel $\varpi : \mathrm{SU}_2(\mathbb{C}) \to \mathrm{SO}_3(\mathbb{R})$, qui est presque un isomorphisme, on dresse au cas par cas la liste des sous-groupes finis de $\mathrm{SU}_2(\mathbb{C})$, puis l'on calcule simultanément la table des caractères de ces sous-groupes et la correspondance de façon explicite.

Que des objets modernes et sophistiqués comme les « groupes de Lie compacts », les « carquois de type de représentation fini » ou les « algèbres amassées de type fini » soient classés par les omniprésents solides platoniciens, c'est tellement beau que, franchement, c'est quand même bien dommage que le vieux Platon ne soit pas là pour voir ça.

1. Relèvement de $SO_3(\mathbb{R})$ à $SU_2(\mathbb{C})$

1.1. Une surjection exceptionnelle

On sait qu'il existe un isomorphisme exceptionnel $SU_2(\mathbb{C})/\{\pm I_2\} \to SO_3(\mathbb{R})$, voir [H2G2, §VII-3]. Précisons un peu. Dans l'exercice ci-dessous, on revient sur le morphisme $\varpi : SU_2(\mathbb{C}) \to SO_3(\mathbb{R})$ induit par l'action par conjugaison de $SU_2(\mathbb{C})$ sur son algèbre de Lie, l'espace des matrices anti-hermitiennes de trace nulle :

$$\mathfrak{su}_2(\mathbb{C}) = \left\{ \begin{pmatrix} ia & b+ic \\ -b+ic & -ia \end{pmatrix}, \ (a,b,c) \in \mathbb{R}^3 \right\}.$$

C'est ce morphisme ϖ, qui par passage au quotient donne l'isomorphisme exceptionnel, que nous allons utiliser dans la suite pour relever les sous-groupes finis de $SO_3(\mathbb{R})$ en sous-groupes (finis également) de $SU_2(\mathbb{C})$. Il n'est pas extravagant d'appeler *groupes binaires* les sous-groupes finis de $SU_2(\mathbb{C})$, par référence aux sous-groupes de $SO_3(\mathbb{R})$, dont ils sont un relèvement « binaire ».

On notera $z = -I_2$ l'unique élément central non trivial de $SU_2(\mathbb{C})$.

Exercice. *On veut montrer que l'action par conjugaison de* $SU_2(\mathbb{C})$ *sur son algèbre de Lie, l'espace* $\mathscr{AH}$ *des matrices anti-hermitiennes de trace nulle, induit le revêtement* $SU_2(\mathbb{C}) \to SO_3(\mathbb{R})$. *On reprend en fait, pas à pas, la preuve de [H2G2, proposition IX-2.1].*

1. *Montrer que* $SU_2(\mathbb{C})$ *agit bien par conjugaison sur* $\mathscr{AH}$.
   On peut le montrer directement, ou utiliser plus savamment le fait que $\mathscr{AH}$ est bien l'algèbre de Lie de $SU_2(\mathbb{C})$ et que donc, le groupe agit par conjugaison sur son algèbre de Lie, [H2G2, lemme IX-A.5.1 et proposition IX-B.5].
2. *Montrer que l'action* $SU_2(\mathbb{C})$ *stabilise le déterminant et en déduire un morphisme* ϖ *de* $SU_2(\mathbb{C})$ *dans* $SO_3(\mathbb{R})$.
3. *Montrer que le noyau de* ϖ *est réduit aux homothéties de* $SU_2(\mathbb{C})$, *c'est-à-dire* $\{\pm I_2\}$.
4. *Montrer que la différentielle de* ϖ *est injective, puis surjective (pour une raison de dimension).*
5. *En déduire que l'isomorphisme* $SU_2(\mathbb{C})/\{\pm I_2\} \to SO_3(\mathbb{R})$ *est bien induit par l'action de* $SU_2(\mathbb{C})$ *sur son algèbre de Lie.*

1.2. Relèvement des éléments

Avant de calculer l'image réciproque d'un sous-groupe par la projection ϖ, on prend un élément à la fois.

1.3. Lemme

(i) *Soit α un réel. L'image réciproque d'une rotation d'angle α est une classe modulo* $\ker\varpi$ *conjuguée à la classe*[1] $\{\pm\mathrm{diag}(\zeta,\zeta^{-1})\}$, *où* $\zeta = e^{i\alpha/2}$.

En particulier, g et zg ne sont pas conjugués dans $SU_2(\mathbb{C})$, *sauf si* $\alpha \in (2\mathbb{Z}+1)\pi$, *c'est-à-dire si la rotation est un demi-tour.*

(ii) *Soit γ un élément d'ordre fini n de* $SO_3(\mathbb{R})$. *Les antécédents de γ sont :*

- *l'un d'ordre $2n$, l'autre d'ordre n si n est impair,*
- *tous deux d'ordre $2n$ si n est pair.*

(iii) *Soit G un sous-groupe cyclique d'ordre n de* $SO_3(\mathbb{R})$ *: alors, $\varpi^{-1}(G)$ est cyclique d'ordre $2n$.*

Démonstration. (i) Soit θ un réel et soit

$$h = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad \text{où } \zeta = e^{i\theta}.$$

Calculons $\varpi(h)$. Pour $(a,b,c) \in \mathbb{R}^3$, l'action de h est donc donnée par :

$$h\cdot\begin{pmatrix} ia & b+ic \\ -b+ic & -ia \end{pmatrix} = h\begin{pmatrix} ia & b+ic \\ -b+ic & -ia \end{pmatrix}h^{-1} = \begin{pmatrix} ia & \zeta^2(b+ic) \\ \zeta^{-2}(-b+ic) & -ia \end{pmatrix}.$$

Alors, $\varpi(h)$ est la matrice de l'action de h dans la base de $\mathfrak{su}_2(\mathbb{C})$ formée des *matrices de Pauli*

$$\left(\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\right).$$

On reconnaît, après calcul une rotation d'angle 2θ :

$$\varpi(h) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos 2\theta & -\sin 2\theta \\ 0 & \sin 2\theta & \cos 2\theta \end{pmatrix}.$$

À présent, soit γ une rotation d'angle α de $SO_3(\mathbb{R})$. Pour κ, élément convenable de $SO_3(\mathbb{R})$, $\kappa^{-1}\gamma\kappa$ est la matrice de rotation précédente, avec $2\theta = \alpha$. Soit k un antécédent de κ par ϖ : alors, $\gamma = \varpi(khk^{-1})$, où h est la matrice ci-dessus. Les antécédents de γ sont donc $g = khk^{-1}$ et $zg = k(zh)k^{-1}$.

(ii) Un élément d'ordre n de $SO_3(\mathbb{R})$ est une rotation d'angle $2k\pi/n$, pour k premier avec n. Ses antécédents ont pour valeurs propres $\exp(\pm ik\pi/n)$ et $\exp(\pm i(k+n)\pi/n)$. Déterminons leurs ordres.

Pour p entier et q entier naturel non nul, l'ordre de $\exp(i\pi p/q)$ est clairement $2q/\operatorname{pgcd}(p,2q)$. Supposons n pair. Nécessairement, k est impair, de

[1] Ici, $\mathrm{diag}(\zeta,\zeta^{-1})$ est la matrice diagonale dont les coefficients diagonaux sont ζ et ζ^{-1}.

même que $k+n$, de sorte que

$$\mathrm{pgcd}(k,2n) = \mathrm{pgcd}(k,n) = 1 = \mathrm{pgcd}(k+n,n) = \mathrm{pgcd}(k+n,2n)\,,$$

et les deux antécédents sont d'ordre $2n$. Supposons n impair. Si k est pair, $k = 2\ell$, on a : $\mathrm{pgcd}(k,2n) = 2\,\mathrm{pgcd}(\ell,n) = 2$; d'autre part, $k+n$ est impair, donc $\mathrm{pgcd}(k+n,2n) = \mathrm{pgcd}(k+n,n) = 1$, si bien que les antécédents sont d'ordres respectifs n et $2n$. Le cas où k est impair est analogue.

(iii) Le groupe cyclique G est engendré par une rotation d'angle $2\pi/n$, dont l'un au moins des antécédents est d'ordre $2n$. Le cardinal de $\varpi^{-1}(G)$ est le double de celui de G, donc $\varpi^{-1}(G)$ est cyclique. □

1.4. Relèvement des classes de conjugaison

Vu que l'on veut dresser la table des caractère de $\tilde{G}$, il faut décrire ses classes de conjugaison. Il s'agit de comprendre le phénomène de *fusion* : des éléments non conjugués dans $\tilde{G}$ peuvent avoir des images conjuguées dans G. On vient d'ailleurs de le constater : si $g \in \mathrm{SU}_2(\mathbb{C})$ est d'ordre impair, alors $-g$ est d'ordre pair et ne lui est pas conjugué ; en revanche, tous deux ont la même image par ϖ. Ici, c'est assez facile, car le noyau de ϖ est seulement d'ordre 2.

1.5. Lemme. *Soit G un sous-groupe fini de $\mathrm{SO}_3(\mathbb{R})$ et soit $\tilde{G} = \varpi^{-1}(G)$. Pour une classe de conjugaison C de G, on note $\tilde{C}$ la partie $\varpi^{-1}(C)$. Soit g dans $\tilde{C}$.*

(i) *Tout élément de $\tilde{G}$ est conjugué à g ou à zg.*

(ii) *Selon que g et zg sont conjugués ou pas, $\tilde{C}$ est une classe ou la réunion de deux classes de conjugaison de $\tilde{G}$.*

(iii) *Soit n l'ordre des éléments de C :*

- *si $n = 2$, $\tilde{C}$ est la réunion d'une ou deux classes d'éléments d'ordre 4 (cela dépend de G) ;*
- *si n est pair et $n \geqslant 4$, $\tilde{C}$ est la réunion de deux classes de conjugaison d'éléments d'ordre $2n$;*
- *si n est impair, $\tilde{C}$ est la réunion d'une classe de conjugaison d'éléments d'ordre $2n$ et d'une classe d'éléments d'ordre n.*

Démonstration. (i) Soit h un élément de $\tilde{C}$. Alors, $\varpi(h)$ et $\varpi(g)$ sont conjugués par un élément $\varpi(k)$, $k \in \tilde{G}$:

$$\varpi(h) = \varpi(k)\varpi(g)\varpi(k)^{-1} = \varpi(kgk^{-1}).$$

Par suite, on a : $h = kgk^{-1}$ ou $h = zkgk^{-1} = k(zg)k^{-1}$, de sorte que h est conjugué à g ou à zg.

L'assertion (ii) en découle immédiatement.

En vertu du lemme 1.3 (i), g et zg appartiennent à des classes de conjugaison distinctes (car $n \neq 2$). La dernière assertion de (iii) est une conséquence de (ii). □

1.6. Classification des sous-groupes finis de $SU_2(\mathbb{C})$

On peut désormais décrire la classification. La clé, c'est que comme le noyau de ϖ est petit, un sous-groupe $\tilde{G}$ de $SU_2(\mathbb{C})$ ne peut pas être très différent de sa saturation $\varpi^{-1}(\varpi(\tilde{G}))$.

1.7. Proposition. *Soit $\varpi : SU_2(\mathbb{C}) \to SO_3(\mathbb{R})$ le morphisme exceptionnel précédent. Un sous-groupe fini de $SU_2(\mathbb{C})$ est conjugué à l'un des suivants :*

- *(type A_{n-1}, $n \in \mathbb{N} \setminus \{0\}$) le groupe cyclique $\mathfrak{C}_n$ d'ordre n engendré par*

$$\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}, \quad \text{où } \xi = e^{2i\pi/n},$$

- *(type D_{n+2}, $n \in \mathbb{N} \setminus \{0,1\}$) le groupe binaire diédral*[2] *$\mathfrak{D}_n$ d'ordre $4n$ engendré par*

$$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ et } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \text{où } \zeta = e^{i\pi/n},$$

- *(type E_6) le groupe $\tilde{\mathfrak{A}}_4$, image inverse par ϖ « du » groupe du tétraèdre,*
- *(type E_7) le groupe $\tilde{\mathfrak{S}}_4$, image inverse par ϖ « du » groupe du cube,*
- *(type E_8) le groupe $\tilde{\mathfrak{A}}_5$, image inverse par ϖ « du » groupe de l'icosaèdre.*

Démonstration. Soit $\tilde{G}$ un sous-groupe fini de $SU_2(\mathbb{C})$. Notons $G = \varpi(\tilde{G})$: c'est un sous-groupe de $SO_3(\mathbb{R})$ et son cardinal est égal à $|\tilde{G}|$ (si $\tilde{G}$ ne contient pas $-I_2$) ou à $|\tilde{G}|/2$ (si $\tilde{G}$ contient $-I_2$). Le groupe « saturé » $\varpi^{-1}(G)$ contient $\tilde{G}$ et son cardinal vaut : $|\varpi^{-1}(G)| = 2|G|$. Ainsi :

- si $-I_2 \in \tilde{G}$, alors $\tilde{G} = \varpi^{-1}(G)$;
- si $-I_2 \notin \tilde{G}$, alors $\tilde{G}$ est un sous-groupe d'indice 2 de $\varpi^{-1}(G)$.

Remarquons que le seul élément d'ordre 2 de $SU_2(\mathbb{C})$ est $-I_2$, générateur de $\ker \varpi$. En effet, un tel élément est diagonalisable et l'une de ses valeurs propres est 1 ou -1, si bien que l'autre aussi puisque leur produit vaut 1. Par suite, en vertu du lemme 1.3 (ii), si $\varpi(\tilde{G})$ contient un élément d'ordre 2, alors $\tilde{G}$ contient un élément d'ordre 4, dont le carré est $-I_2$: en d'autres termes, si $|G|$ est pair, $\tilde{G}$ contient $-I_2$.

Premier cas. Supposons que $|\tilde{G}|$ soit impair. On en déduit que $-I_2$ n'est pas dans $\tilde{G}$, et que $\tilde{G}$ est donc isomorphe à G. D'après la classification des sous-groupes de $SO_3(\mathbb{R})$, voir le théorème IX-3.12, on en déduit que G, d'ordre

[2] Attention à ne pas confondre ce groupe avec le groupe diédral.

impair, est nécessairement cyclique. D'après le lemme 1.3 (iii), $\varpi^{-1}(G)$ est un groupe cyclique d'ordre $2n$, il contient un unique sous-groupe d'ordre n : c'est $\tilde{G}$.

Deuxième cas. Supposons que $|\tilde{G}|$ soit pair, et donc $-\mathrm{I}_2 \in \tilde{G}$, si bien que $\tilde{G}$ est l'image réciproque de G par ϖ. Si G est cyclique, le lemme 1.3 (iii) indique que $\tilde{G}$ est cyclique d'ordre $2|G|$. Si G est le groupe de symétrie d'un polyèdre régulier, alors $|G|$ est pair, et $\tilde{G} = \varpi^{-1}(G)$ tombe donc dans l'un des types appelés E_6, E_7 et E_8.

Pour terminer la preuve, il suffit de vérifier que le groupe engendré par

$$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \text{où } \zeta = e^{i\pi/n},$$

est l'image réciproque d'un groupe diédral (donc d'ordre pair !). Pour cela, on peut par exemple vérifier que ce groupe est le groupe à $4n$ éléments formé des matrices monomiales[3] de déterminant 1 dont les coefficients sont des racines $2n$-ièmes de l'unité et calculer son image par ϖ. □

2. Produit tensoriel et graphe de McKay d'un sous-groupe fini de $\mathrm{SU}_2(\mathbb{C})$

Suivant McKay [53], [54], on va associer un graphe à un sous-groupe fini G de $\mathrm{SU}_2(\mathbb{C})$, que l'on choisira non trivial pour des raisons hautement ésotériques. L'inclusion de $\mathrm{SU}_2(\mathbb{C})$ dans $\mathrm{GL}_2(\mathbb{C})$ fournit une représentation fidèle, dite *standard*, de degré 2, à savoir : $\rho_{\mathrm{std}} : G \to \mathrm{GL}_2(\mathbb{C})$, $g \mapsto g$. On note χ_{std} son caractère.

Pour χ et χ' dans $\mathrm{Irr}(G)$, on note $n_{\chi\to\chi'}$ la multiplicité de χ' dans le produit tensoriel de χ par χ_{std} :

$$n_{\chi\to\chi'} = \langle \chi\chi_{\mathrm{std}}, \chi' \rangle,$$

En mettant $n_{\chi\to\chi'}$ flèches de χ vers χ', on ferait de l'ensemble des caractères irréductibles de $\tilde{G}$ un graphe orienté. La propriété de symétrie suivante permet d'oublier l'orientation. Elle provient du fait que la représentation standard est isomorphe à sa duale, et cela vient du fait que les éléments de $\tilde{G}$ ont pour déterminant 1.

2.1. Proposition. *Pour tous caractères irréductibles χ et χ', on a :*

$$n_{\chi\to\chi'} = n_{\chi'\to\chi}.$$

[3] Il peut être utile de rappeler que les matrices monomiales sont des matrices de permutation où les « 1 » sont remplacés par des scalaires non nuls.

Démonstration. Par définition, la composante connexe de la représentation triviale est formée des caractères qui apparaissent dans une des puissances tensorielles de la représentation naturelle $\mathbb{C}^2$. La proposition A.8 indique que l'on y trouve tous les caractères.

L'égalité repose sur le fait que la trace d'un élément d'ordre fini de $\mathrm{SU}_2(\mathbb{C})$ est réelle (c'est $\zeta + \zeta^{-1} = \zeta + \overline{\zeta}$ pour une racine de l'unité ζ). Par suite, pour χ et χ' caractères irréductibles :

$$n_{\chi\to\chi'} = \langle \chi\chi_{\mathrm{std}}, \chi' \rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\chi(g)\chi_{\mathrm{std}}(g)}\chi'(g)$$
$$= \frac{1}{|G|} \sum_{g\in G} \overline{\chi(g)}\chi_{\mathrm{std}}(g)\chi'(g) = \overline{n_{\chi'\to\chi}} = n_{\chi'\to\chi},$$

la dernière égalité venant du fait qu'un produit scalaire de caractères est un entier. □

2.2. Définition. Le *graphe de McKay* associé à un sous-groupe fini G de $\mathrm{SU}_2(\mathbb{C})$ est un graphe non orienté défini ainsi :
- l'ensemble des sommets du graphe est l'ensemble $\mathrm{Irr}(G)$ des caractères irréductibles de G ;
- pour χ et χ' dans $\mathrm{Irr}(G)$, le nombre d'arêtes entre χ et χ' est le nombre $n_{\chi\to\chi'}$, défini ci-dessus.

2.3. Proposition. *Le graphe de McKay d'un sous-groupe de* $\mathrm{SU}_2(\mathbb{C})$ *est connexe,* i.e. *toute paire de sommets est reliée par une suite d'arêtes.*

Démonstration. Par définition, la composante connexe de la représentation triviale est formée des caractères qui apparaissent dans une des puissances tensorielles de la représentation naturelle $\mathbb{C}^2$. La proposition A.8 indique que l'on y trouve tous les caractères. D'où la connexité. □

Il sera utile et élégant de remarquer que le groupe $\mathrm{Mor}(\tilde{G}, \mathbb{C}^*)$ des caractères linéaires de $\tilde{G}$ agit sur le graphe de McKay qui lui est associé. Par « *agir sur un graphe* », on entend ici que le groupe agit sur l'ensemble des sommets et sur l'ensemble des arêtes du graphe de sorte que si S, S' sont deux sommets reliés par une arête α, et et si g appartient au groupe, alors $g \cdot S$ et $g \cdot S'$ sont reliés par l'arête $g \cdot \alpha$. Dans le cas des graphes finis que l'on manipule ici, cela revient à dire que le nombre d'arêtes reliant la paire de sommets $\{S, S'\}$ est invariant par le groupe.

2.4. Proposition. *Pour tout sous-groupe fini* $\tilde{G}$ *de* $\mathrm{SU}_2(\mathbb{C})$, *l'action par tensorisation sur les caractères induit une action du groupe* $\mathrm{Mor}(\tilde{G}, \mathbb{C}^*)$ *sur le graphe de McKay de* $\tilde{G}$.

Démonstration. On a vu dans l'exercice X-F.25 que $\mathrm{Mor}(\tilde{G}, \mathbb{C}^*)$ agit sur l'ensemble $\mathrm{Irr}(\tilde{G})$ des caractères de $\tilde{G}$ par produit : $\varepsilon \cdot \chi = \varepsilon\chi$. Il suffit donc de voir que le nombre d'arêtes qui relient la paire $\{\chi, \chi'\} \subset \mathrm{Irr}(\tilde{G})$ ne varie pas pour l'action de $\tilde{G}$. En effet, pour tout ε de $\mathrm{Mor}(\tilde{G}, \mathbb{C}^*)$, on a :

$$n_{\varepsilon\chi \to \varepsilon\chi'} = \langle \varepsilon\chi\chi_{\mathrm{std}}, \varepsilon\chi' \rangle = \langle \chi\chi_{\mathrm{std}}, \bar{\varepsilon}\varepsilon\chi' \rangle = \langle \chi\chi_{\mathrm{std}}, \chi' \rangle = n_{\chi \to \chi'}. \qquad \square$$

2.5. Remarque. On peut se demander si les autres groupes connus pour agir sur $\mathrm{Irr}(\tilde{G})$, c'est-à-dire $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, voir l'exercice X-F.23, et $\mathrm{Out}(\tilde{G})$, voir l'exercice X-F.24, agissent également sur le graphe de McKay de $\tilde{G}$. On peut facilement remarquer (et l'on en fera les frais pour E_8) que non. En fait, c'est le stabilisateur de χ_{std}, pour l'action considérée, qui agit sur le graphe de McKay de $\tilde{G}$. On constatera au cas par cas que ces actions sont soit triviales, soit font double emploi avec l'action de $\mathrm{Mor}(\tilde{G}, \mathbb{C}^*)$ définie ci-dessus.

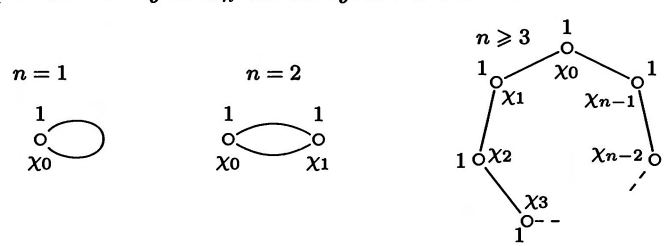
3. Groupes cycliques

On sait, ou l'on devine aisément, ce que peut être un graphe à n sommets, $n \geqslant 2$. Cela demande tout de même quelques précisions pour $n = 2$: on dit qu'il s'agit du graphe dont les deux sommets sont reliés par deux arêtes.

3.1. Proposition. *Soit n un entier non nul et soit $\mathfrak{C}_n$ le groupe engendré par*

$$C_\xi = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}, \quad \text{où } \xi = e^{2i\pi/n}.$$

Le graphe de McKay de $\mathfrak{C}_n$ est un cycle à n sommets[4] *:*



Démonstration. Pour $k \in \mathbb{Z}$, on note χ_k le caractère défini par $\mathfrak{C}_n \to \mathbb{C}^*$, $C_\xi \mapsto \xi^k$. Bien sûr, si $k \equiv k' \pmod{n}$, on a : $\chi_k = \chi_{k'}$, ce qui nous permet de considérer k dans $\mathbb{Z}/n\mathbb{Z}$. Le caractère χ_{std} de la représentation naturelle

[4] Les lettres grecques sont les noms des caractères introduits ci-dessous ; les nombres désignent leur degré.

de $\mathfrak{C}_n$ est : $\chi_{\text{std}} = \chi_1 + \chi_{-1}$. Si $n > 2$, vu que $\chi_{\pm 1}\chi_k = \chi_{k\pm 1}$, on en déduit que χ_k est relié à $\chi_{k\pm 1}$, ce qui définit exactement le cycle à n sommets.

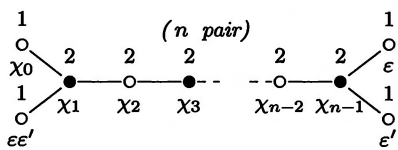
On vérifie ensuite sans encombre les deux cas particuliers $n = 1$, $n = 2$. □

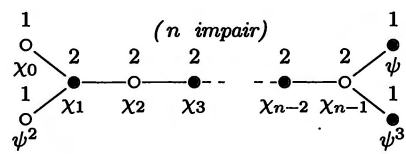
4. Groupes binaires diédraux

Soit n un entier supérieur ou égal[5] à 2. On note $\tilde{\mathfrak{D}}_n$ le groupe *binaire diédral*[6] d'ordre $4n$ engendré par

$$r = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \quad \text{et} \quad s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \text{où } \zeta = e^{i\pi/n}.$$

4.1. Proposition. *Soit n entier supérieur à 2. Le graphe de McKay du groupe binaire diédral $\tilde{\mathfrak{D}}_n$ est*[7] *:*





4.2. Lemme. *(Notations ci-dessus.)*

(i) *Dans le groupe $\tilde{\mathfrak{D}}_n$, on a les relations :*

$$r^n = s^2 = z \text{ (élément central)}, \quad srs^{-1} = r^{-1}.$$

(ii) *Tout élément de $\tilde{\mathfrak{D}}_n$ peut s'écrire de façon unique $s^k r^\ell$ (avec $k \in \{0,1\}$ et $\ell \in \{0,\dots,2n-1\}$).*

(iii) *Les $n+3$ classes de conjugaison de $\tilde{\mathfrak{D}}_n$ sont :*

$$\begin{cases} C(r^\ell) = \{r^\ell, r^{-\ell}\} \quad (\ell \in \{0,\dots,n\}), \\ C(s) \;\; = \{sr^k,\ k \equiv 0 \pmod 2\}, \\ C(sr) = \{sr^k,\ k \equiv 1 \pmod 2\}. \end{cases}$$

(iv) *Le groupe dérivé $[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ de $\tilde{\mathfrak{D}}_n$ est d'indice 4, engendré par r^2. Si n est pair, $\tilde{\mathfrak{D}}_n/[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$; si n est impair, $\tilde{\mathfrak{D}}_n/[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ est isomorphe au groupe cyclique $\mathbb{Z}/4\mathbb{Z}$.*

[5] Pour $n = 1$, le groupe serait cyclique d'ordre 4, engendré par s.

[6] Quitte à le répéter, ce groupe n'est pas le groupe diédral, dont nous laissons en exercice la table des caractères.

[7] Les lettres grecques sont les noms des caractères introduits ci-dessous ; les nombres désignent leur degré. Les points blancs désignent les caractères du quotient par $\langle z \rangle$.

Démonstration. (ii) Soit g un élément de $\tilde{\mathfrak{D}}_n$ différent de l'identité : c'est un produit de puissances de r et de s, puissances que l'on peut supposer positives puisque r et s sont d'ordre fini :

$$g = s^{k_1} r^{\ell_1} s^{k_2} r^{\ell_2} \cdots s^{k_p} r^{\ell_p}, \quad p \in \mathbb{N}^*,\ k_1, \ell_1, \ldots, k_p, \ell_p \in \mathbb{N}.$$

On appelle poids d'une telle écriture la somme $k_1 + \cdots + k_p$. Parmi toutes les écritures de cette forme, choisissons-en une de poids minimal. Montrons que ce poids est 0 ou 1.

Tous les k_i valent 0 ou 1. En effet, si l'on a : $k_i = k_i' + 2q_i$ avec $k_i' \in \{0, 1\}$ et q_i entier, on écrit : $s^{k_i} r^{\ell_i} = s^{k_i'} s^{2q_i} r^{\ell_i} = s^{k_i'} r^{nq_i + \ell_i}$: par minimalité du poids de l'écriture choisie, $k_1 + \cdots + k_p \leqslant k_1' + \cdots + k_p'$ alors que $k_i' \leqslant k_i$ pour tout i : ainsi, $k_i = k_i'$ pour tout i.

De plus, la minimalité du poids assure qu'au plus un des coefficients k_i vaut 1 : en effet, si deux exposants de s valaient 1, on pourrait remplacer $sr^{\ell}s$ par $r^{-\ell}$, ce qui donnerait une écriture de poids strictement plus petite. Ainsi, une écriture avec un nombre de blocs minimal est de la forme $s^{k_1} r^{\ell_1}$ ou $r^{\ell_1} s r^{\ell_2} = s r^{-\ell_1 + \ell_2}$, ce qui prouve l'existence dans l'assertion (ii). L'unicité résulte du fait que les sous-groupes engendrés respectivement par r et par s sont d'intersection triviale.

(iii) Soit $\ell \in \{0, \ldots, 2n-1\}$. On a :

$$\begin{cases} r\, r^{\ell}\, r^{-1} = r^{\ell} \\ s\, r^{\ell}\, s^{-1} = r^{-\ell} \end{cases} \quad \text{et} \quad \begin{cases} r\, s r^{\ell}\, r^{-1} = s r^{\ell - 2}, \\ s\, s r^{\ell}\, s^{-1} = s r^{-\ell}. \end{cases}$$

Comme r et s engendrent $\tilde{\mathfrak{D}}_n$, on en déduit que r^{ℓ} est conjugué à $r^{\ell'}$ si et seulement si $\ell \equiv \pm \ell' \pmod{2n}$ et que sr^{ℓ} est conjugué à $sr^{\ell'}$ si et seulement si $\ell \equiv \pm \ell' \pmod{2n}$ ou $\ell \equiv \ell' \pmod{2}$; comme $2n$ est pair, cela revient à dire que ℓ et ℓ' ont la même parité.

(iv) Soient $\ell, \ell' \in \{0, \ldots, 2n-1\}$. On calcule les commutateurs non triviaux :

$$[r^{\ell}, sr^{\ell'}] = r^{\ell} s r^{\ell'} r^{-\ell} r^{-\ell'} s^{-1} = r^{\ell} s r^{-\ell} s^{-1} = r^{2\ell},$$

$$[sr^{\ell}, sr^{\ell'}] = sr^{\ell} sr^{\ell'} r^{-\ell} s^{-1} r^{-\ell'} s^{-1} = sr^{2\ell - 2\ell'} s^{-1} = r^{2(\ell' - \ell)}.$$

Il en résulte que $[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ est engendré par r^2 ; il est donc d'ordre n et le groupe $[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ est d'ordre 4. Si n est pair, ce groupe contient $r^n = s^2$, si bien que les classes de r et s sont d'ordre 2 dans le quotient $\tilde{\mathfrak{D}}_n / [\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$. Si n est impair, le groupe $[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ ne contient pas r^n et donc s est d'ordre 4 dans le quotient. □

On cherche à présent la table des caractères des groupes binaires diédraux. Il y a des méthodes plus simples pour le faire, mais ici, le but est de calculer aussi le graphe de McKay. On procède de façon récursive des caractères en tensorisant chaque caractère obtenu par le caractère standard.

4.3. Proposition. *Soit n un entier, $n \geqslant 2$. La table des caractères de $\tilde{\mathfrak{D}}_n$ est donnée comme suit :*

n pair :

card classe	1 e	1 z	2 r^ℓ $(1 \leqslant \ell < n)$	n s	n sr
χ_0	1	1	1	1	1
ε	1	1	$(-1)^\ell$	-1	1
ε'	1	1	$(-1)^\ell$	1	-1
$\varepsilon\varepsilon'$	1	1	1	-1	-1
χ_k $(1 \leqslant k < n)$	2	$(-1)^k 2$	$2\cos\frac{k\ell\pi}{n}$	0	0

n impair :

card classe	1 1	1 z	2 r^ℓ $(1 \leqslant \ell < n)$	n s	n sr
χ_0	1	1	1	1	1
ψ	1	-1	$(-1)^\ell$	i	$-i$
ψ^2	1	1	1	-1	-1
ψ^3	1	-1	$(-1)^\ell$	$-i$	i
χ_k $(1 \leqslant k < n)$	2	$(-1)^k 2$	$2\cos\frac{k\ell\pi}{n}$	0	0

Démonstration. L'hypothèse sur n assure que la représentation standard est irréductible. Construisons la table des caractères petit à petit en partant du caractère trivial χ_0.

card classe	1 1	1 z	2 r^ℓ	n s	n sr
χ_0 (trivial)	1	1	1	1	1

Il est commode de disposer des caractères linéaires, *i.e.* de degré 1, de $\tilde{\mathfrak{D}}_n$. Ce sont les représentations du groupe abélien $\tilde{\mathfrak{D}}_n/[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ qui, d'après le lemme 4.2, est d'ordre 4.

Lorsque n est pair, $\tilde{\mathfrak{D}}_n/[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ est le groupe de Klein, engendré par les classes de s et de r. On détermine un caractère linéaire en choisissant arbitrairement sa valeur en s et en r, ce qui donne, en composant le caractère de $\tilde{\mathfrak{D}}_n/[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ par la surjection canonique $\tilde{\mathfrak{D}}_n \to \tilde{\mathfrak{D}}_n/[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$, les quatre caractères ε, ε' et $\varepsilon\varepsilon'$ ci-dessous.

n pair :

card classe	1 e	1 z	2 r^ℓ $(1 \leqslant \ell < n)$	n s	n sr
χ_0	1	1	1	1	1
ε	1	1	$(-1)^\ell$	-1	1
ε'	1	1	$(-1)^\ell$	1	-1
$\varepsilon\varepsilon'$	1	1	1	-1	-1

Lorsque n est impair, $\tilde{\mathfrak{D}}_n/[\tilde{\mathfrak{D}}_n, \tilde{\mathfrak{D}}_n]$ est cyclique d'ordre 4, engendré par la

classe de s ; la classe de r est égale à celle de s. Un caractère linéaire est donc déterminé par sa valeur en s parmi $\{\pm 1, \pm i\}$.

n impair :

card classe	1 1	1 z	2 r^ℓ $(1 \leqslant \ell < n)$	n s	n sr
χ_0	1	1	1	1	1
ψ	1	-1	$(-1)^\ell$	i	$-i$
ψ^2	1	1	1	-1	-1
ψ^3	1	-1	$(-1)^\ell$	$-i$	i

Notons $\chi_1 = \chi_{\text{std}}$ le caractère de la représentation naturelle. La ligne correspondante de la table des caractères est :

classe	1	z	r^ℓ $(1 \leqslant \ell < r)$	s	sr
$\chi_1 = \chi_{\text{std}}$	2	-2	$2\cos\frac{\ell\pi}{n}$	0	0

Avant de chercher inductivement les derniers caractères, nous allons noter $\phi = \varepsilon\varepsilon'$ pour le cas pair et $\phi = \psi^2$ pour le cas impair, ce qui permet de traiter les deux cas simultanément. Par exemple, on a : $\phi\chi_{\text{std}} = \chi_{\text{std}}$: cela traduit une action triviale de $\phi \in \text{Mor}(\tilde{\mathfrak{D}}_n, \mathbb{C}^*)$ sur χ_{std} (proposition 2.4).

On a bien évidemment $\chi_0\chi_{\text{std}} = \chi_{\text{std}}$. On va donc décomposer le caractère χ_1^2 en irréductibles tout en sachant, proposition 2.1, que le caractère trivial apparaît avec multiplicité 1 dans χ_1^2. On peut calculer la norme de χ_1^2 ; on trouve : $\langle \chi_1^2, \chi_1^2 \rangle = 3$, ce qui signifie que χ_1^2, caractère de degré $2^2 = 4$, est somme de trois irréductibles : l'un est le caractère trivial, les autres sont de dimensions respectives 1 et 2.

Comme l'action de ϕ stabilise χ_{std}, le fait que χ_{std} et χ_0 sont reliées par une arête implique que $\phi\chi_{\text{std}} = \chi_{\text{std}}$ et $\phi\chi_0 = \phi$ sont reliées par une arête. Donc, ϕ est aussi dans la décomposition de χ_{std}^2.

On en déduit que $\chi_1^2 - \chi_0 - \phi$ est un caractère irréductible de degré 2. On le note χ_2 ; il se calcule grâce à la formule du cosinus de l'angle moitié :

classe	1	z	r^ℓ $(1 \leqslant \ell < r)$	s	sr
$\chi_2 = \chi_1^2 - \chi_0 - \phi$	2	2	$2\cos\frac{2\ell\pi}{n}$	0	0

Comme χ_2 apparaît dans χ_1^2, on sait que χ_1 apparaît dans $\chi_2\chi_1$, voir la proposition 2.1. Observons la classe de r^ℓ.

$$\chi_2\chi_1(r^k) = 4\cos\frac{2\ell\pi}{n}\cos\frac{\ell\pi}{n} = 2\cos\frac{\ell\pi}{n} + 2\cos\frac{3\ell\pi}{n} = \chi_1(r^k) + 2\cos\frac{3\ell\pi}{n}.$$

On calcule ainsi la différence $\chi_3 = \chi_2\chi_1 - \chi_1$.

classe	1	z	r^ℓ $(1 \leqslant \ell < r)$	s	sr
$\chi_3 = \chi_2\chi_1 - \chi_1$	2	-2	$2\cos\frac{3\ell\pi}{n}$	0	0

Un calcul de produit scalaire prouve que χ_3 est irréductible. On voit bien comment continuer : pour $k \geqslant 1$, définissons la fonction centrale χ_k par :

classe	1	z	r^ℓ $(1 \leqslant \ell < r)$	s	sr
χ_k	2	$(-1)^k 2$	$2\cos\frac{k\ell\pi}{n}$	0	0

On montre avec un peu de trigonométrie que l'on a, pour tout k :

$$\chi_k\chi_1 = \chi_{k-1} + \chi_{k+1}. \qquad (E_k)$$

En effet, cette égalité résume les suivantes :

$$\chi_k\chi_1(e) = 2 \times 2 = 2 + 2 = \chi_{k-1}(e) + \chi_{k+1}(e);$$

$$\chi_k\chi_1(z) = (-1)^k 2 \times (-2) = (-1)^{k-1}2 + (-1)^{k+1}2 = \chi_{k-1}(e) + \chi_{k+1}(e);$$

$$\begin{aligned}\chi_k\chi_1(r^\ell) &= 4\cos\frac{k\ell\pi}{n}\cos\frac{\ell\pi}{n} = 2\cos\frac{(k+1)\ell\pi}{n} + 2\cos\frac{(k-1)\ell\pi}{n}\\ &= \chi_{k-1}(r^\ell) + \chi_{k+1}(r^\ell);\end{aligned}$$

$$\chi_k\chi_1(sr^\ell) = 0 = \chi_{k-1}(sr^\ell) + \chi_{k+1}(sr^\ell).$$

On en déduit, par récurrence, que χ_k est un caractère de $\tilde{\mathfrak{D}}_n$. Supposons que $\chi_1, \ldots, \chi_k$ soient des caractères. La relation (E_{k-1}) entraîne que χ_k apparaît dans le produit tensoriel $\chi_{k-1}\chi_1$, d'où il résulte que χ_{k-1} apparaît dans $\chi_k\chi_1$, voir proposition 2.1, puis que $\chi_{k+1} = \chi_k\chi_1 - \chi_{k-1}$ est un caractère.

On vérifie grâce au produit scalaire que χ_k est irréductible si $1 \leqslant k \leqslant n-1$:

$$\begin{aligned}\langle\chi_k, \chi_k\rangle &= \frac{1}{4n}\Big(2^2 + 2^2 + \sum_{\ell=1}^{n-1} 2\big|\zeta^{k\ell} + \zeta^{-k\ell}\big|^2\Big)\\ &= \frac{1}{4n}\Big(8 + 2\sum_{\ell=1}^{n-1}\big(\zeta^{2k\ell} + 2 + \zeta^{-2k\ell}\big)\Big) = 1.\end{aligned}$$

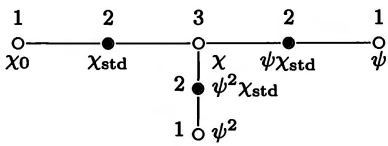
On a ainsi défini quatre caractères linéaires et $n-1$ caractères de degré 2, soit $n+3$ caractères de $\tilde{\mathfrak{D}}_n$: la table des caractères est complète.

Enfin, pour terminer le graphe de McKay, on n'a plus qu'à remarquer sa symétrie à l'aide de l'action de $\mathrm{Mor}(\tilde{\mathfrak{D}}_n, \mathbb{C}^*)$ et que l'orbite de χ_{std} est la paire $\{\chi_1, \chi_{n-1}\}$. □

5. Groupe binaire tétraédral

Soient $G = \mathfrak{A}_4$ le groupe de symétrie d'un tétraèdre régulier et $\tilde{\mathfrak{A}}_4 = \varpi^{-1}(\mathfrak{A}_4)$ le *groupe binaire tétraédral.*

5.1. Proposition. *Le graphe de McKay du groupe binaire tétraédral est*[8] *:*



5.2. Caractères de $\mathfrak{A}_4$

On supposera connues les classes de conjugaison de $\mathfrak{A}_4$, voir section 5.2 :

nom classe	1	2	3_1	3_2
représentant	Id	(12)(34)	(123)	(132)
ordre	1	2	3	3
cardinal	1	3	4	4

Remarquons que la classe 3_2 est formée des carrés — ou des inverses, ce qui revient au même — des éléments de la classe 3_1 — et inversement.

Le groupe de Klein, c'est-à-dire le sous-groupe de $\mathfrak{A}_4$ engendré par les double-transpositions, est distingué. Le quotient par le groupe de Klein est d'ordre 3, donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Il possède donc trois caractères linéaires que l'on notera 1, ψ, ψ^2. En notant classiquement j une racine primitive troisième de l'unité, on trouve :

nom classe	1	2	3_1	3_2
χ_0	1	1	1	1
ψ	1	1	j	j^2
ψ^2	1	1	j^2	j

Comme le groupe $\mathfrak{A}_4$ possède quatre classes de conjugaison et autant de caractères irréductibles, il nous en manque un que l'on notera χ. Il est de degré $(12-1^2-1^2-1^2)^{1/2} = 3$. Comme le produit tensoriel $\psi\chi$ est aussi un caractère de degré 3, automatiquement irréductible (vérifier !), il coïncide avec χ. Par suite, χ s'annule sur les classes où ψ ne prend pas la valeur 1. Puisque χ est orthogonal au caractère trivial, on en déduit la dernière ligne

[8] Mêmes conventions que dans la proposition 4.1.

de la table des caractères de $\mathfrak{A}_4$:

nom classe	1	2	3_1	3_2
représentant	Id	(12)(34)	(123)	(132)
cardinal	1	3	4	4
χ_0	1	1	1	1
ψ	1	1	j	j^2
ψ^2	1	1	j^2	j
χ	3	-1	0	0

Ce n'est pas une surprise : $\mathfrak{A}_4$ est un sous-groupe du groupe orthogonal $\mathrm{SO}_3(\mathbb{R})$ et χ est le caractère correspondant. On peut aussi réaliser cette représentation de la façon suivante. Puisque $\mathfrak{A}_4$ agit sur quatre lettres, on a une action doublement transitive sur quatre éléments, et donc une représentation par permutation de degré 4, qui fournit une représentation irréductible de degré 3.

5.3. Caractères de $\tilde{\mathfrak{A}}_4$

On cherche ici les caractères de représentations irréductibles de $\tilde{\mathfrak{A}}_4$. De l'étude précédente, on connaît déjà des caractères linéaires : le caractère trivial et les caractères d'ordre 3 que l'on appellera encore ψ et ψ^2.

De plus, grâce à l'étude des classes de conjugaison de $\mathfrak{A}_4$, vues en 5.2, on remarque que la classe 3_1 se scinde, par le lemme 1.5 (iii), en deux classes formées d'éléments d'ordres 3 et 6. De même pour 3_2. De plus, la classe triviale de $\mathfrak{A}_4$ se relève en deux classes distinctes. Ainsi, le lemme 1.5 (iii) permet d'affirmer que, selon le comportement de la classe des involutions, $\tilde{\mathfrak{A}}_4$ possède sept ou huit classes de conjugaison.

En tant que sous-groupe de $\mathrm{SU}_2(\mathbb{C})$, $\tilde{\mathfrak{A}}_4$ possède un caractère naturel de degré 2, déjà noté χ_{std}. On détermine χ_{std} grâce au lemme 1.3 : les relèvements d'une rotation d'ordre fini et d'angle θ ont pour valeurs propres $\exp \pm\theta/2$ et $\exp \pm(\theta+\pi)/2$, donc leurs traces sont $2\cos\theta/2$ et $-2\cos\theta/2$.

Pour les classes qui relèvent les éléments d'ordre 3, l'angle de la rotation vaut $\pm 2\pi/3$, donc, en ces éléments, χ_{std} prend la valeur $\pm 2\cos\pi/3 = \pm 1$. Il est important de remarquer que cette valeur ne s'annule pas, ce qui entraîne que les produits tensoriels $\psi\chi_{\mathrm{std}}$ et $\psi\chi_{\mathrm{std}}$ sont distincts de χ_{std}. On met ainsi en évidence, sans effort, que $\tilde{\mathfrak{A}}_4$ possède trois caractères irréductibles de degré 2. Or :

$$\underbrace{1^2+1^2+1^2+3^2}_{\text{caractères de } \mathfrak{A}_4} + \underbrace{2^2+2^2+2^2}_{\text{nouveaux caractères}} = 24 = |\tilde{\mathfrak{A}}_4|,$$

si bien que l'on connaît tous les degrés des caractères de $\tilde{\mathfrak{A}}_4$. En particulier, il ne peut y avoir huit classes de conjugaison, et par ce qui précède, il y a

sept classes de conjugaison. Comme produit dérivé, on obtient donc que la classe des involutions ne se scinde pas dans le relèvement.

On peut compléter la table des caractères : on calcule facilement χ_{std}, puis l'on multiplie par ψ et ψ^2.

nom classe	1	z	$\tilde{2}$	$\tilde{3}_1$	$\tilde{6}_1$	$\tilde{3}_2$	$\tilde{6}_2$
cardinal	1	1	6	4	4	4	4
χ_0	1	1	1	1	1	1	1
ψ	1	1	1	j	j	j^2	j^2
ψ^2	1	1	1	j^2	j^2	j	j
χ	3	3	-1	0	0	0	0
χ_{std}	2	-2	0	1	-1	-1	1
$\psi\chi_{\text{std}}$	2	-2	0	j	$-j$	$-j^2$	j^2
$\psi^2\chi_{\text{std}}$	2	-2	0	j^2	$-j^2$	$-j$	j

5.4. Graphe de McKay de $\tilde{\mathfrak{A}}_4$

Pour écrire le graphe de McKay associé à ce sous-groupe, il faut décomposer les produits tensoriels par χ_{std}. D'évidence, on a : $\chi_0\chi_{\text{std}} = \chi_{\text{std}}$. Ensuite, χ_{std}^2 est somme de deux caractères irréductibles puisque le calcul donne $\langle\chi_{\text{std}}^2, \chi_{\text{std}}^2\rangle = 2$ et que l'un des deux est le caractère trivial, par la proposition 2.1. L'autre est donc χ, l'unique caractère de degré 3. On peut aussi constater que $\chi_{\text{std}}^2 = \chi_0 + \chi\ldots$

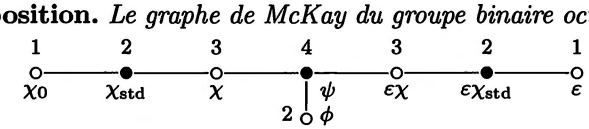
À présent, on souhaite décomposer $\chi\chi_{\text{std}}$. C'est une représentation de degré 6 dans laquelle apparaît χ_{std}, par la proposition 2.1. On sait que χ_{std} est relié à χ, donc χ_{std} intervient dans ce produit. Or, comme on peut le voir sur le tableau, l'action de $\text{Mor}(\tilde{\mathfrak{A}}_4, \mathbb{C}^*) = \{\chi_0, \psi, \psi^2\}$ sur le graphe stabilise le sommet χ, et $\psi\chi_{\text{std}}$, $\psi^2\chi_{\text{std}}$ sont donc aussi reliés à χ par une arête. Et comme $2 + 2 + 2 = 6$, on a ici toutes les arêtes reliées à χ.

Encore une fois, l'action de $\text{Mor}(\tilde{\mathfrak{A}}_4, \mathbb{C}^*)$ sur le graphe permet de conclure la proposition 5.1.

6. Groupe binaire octaédral

Soit $\mathfrak{S}_4$ le groupe de symétries d'un cube et soit $\tilde{\mathfrak{S}}_4 = \varpi^{-1}(\mathfrak{S}_4)$ le *groupe binaire cubique/octaédral.*

6.1. Proposition. *Le graphe de McKay du groupe binaire octaédral est*[9] :



[9]Mêmes conventions que dans la proposition 4.1.

6.2. Description sommaire des caractères de $\mathfrak{S}_4$

Les classes de conjugaison de $\mathfrak{S}_4$ sont indexées par les partitions de 4, voir l'exercice X-C.10 :

nom classe	1	2_1	3	4	2_2
représentant	Id	(12)	(123)	(1234)	(12)(34)
ordre	1	2	3	4	2
cardinal	1	6	8	6	3

Le groupe $\mathfrak{S}_4$ admet donc cinq caractères irréductibles. Voici sa table des caractères :

nom classe	1	2_1	3	4	2_2
représentant	Id	(12)	(123)	(1234)	(12)(34)
cardinal	1	6	8	6	3
χ_0	1	1	1	1	1
ε	1	−1	1	−1	1
χ	3	1	0	−1	−1
$\varepsilon\chi$	3	−1	0	1	−1
ϕ	2	0	−1	0	2

On peut la reconstruire de la façon suivante :

- rien à dire sur le caractère trivial, de degré 1 ;
- rien de plus sur la signature ε, unique[10] caractère non trivial de degré 1 ;
- faire agir $\mathfrak{S}_4$ sur quatre lettres donne une représentation irréductible par la proposition X-B.15 (la double-transitivité est largement assurée) de degré 3 ; on note χ son caractère ;
- le produit tensoriel $\varepsilon\chi$ est un autre caractère de degré 3, comme on le vérifie sur la table ;
- comme il y a cinq classes de conjugaison, il ne reste plus qu'une représentation à trouver : on la déduit des relations d'orthogonalité des colonnes X-C.12 ; on peut aussi la voir comme la représentation associée à l'action de $\mathfrak{S}_4$ sur les trois directions de faces opposées d'un cube, voir [H2G2, exercice XII-C.2].

Au bilan, on a tous les caractères irréductibles puisque la somme des carrés des degrés est :

$$1^2 + 1^2 + 3^3 + 3^3 + 2^2 = 24 = |\mathfrak{S}_4|.$$

[10] Un caractère prend la même valeur en toutes transpositions car elles sont toutes conjuguées ; cette valeur est -1 ou 1 car une transposition est d'ordre 2 ; elle détermine complètement le caractère car le groupe symétrique est engendré par les transpositions.

Passons aux classes de conjugaison. Par le lemme 1.5 (iii), quand on la relève dans $\tilde{\mathfrak{S}}_4$, chaque classe C d'éléments d'ordre o différent de 2 de $\mathfrak{S}_4$ se scinde :

- si $o = 3$, en deux classes $\tilde{C}$ et $\tilde{\tilde{C}}$ formées d'éléments d'ordres respectifs o et $2o$;
- si $o = 4$, en deux classes $\tilde{C}$ et $\tilde{C}'$ formées d'éléments d'ordre $2o$.

Selon le comportement des classes d'involutions, $\tilde{\mathfrak{S}}_4$ possède donc entre huit et dix classes de conjugaison, donc autant de caractères irréductibles. On peut préciser.

6.3. Lemme. *Le groupe $\tilde{\mathfrak{S}}_4$ possède huit classes de conjugaison :*

nom classe	1	z	$\tilde{2}_1$	$\tilde{3}$	$\tilde{\tilde{3}}$	$\tilde{4}$	$\tilde{4}'$	$\tilde{2}_2$
ordre	1	2	4	3	6	8	8	4
cardinal	1	1	12	8	8	6	6	6

Ses huit caractères irréductibles ont pour degrés 1, 1, 2, 2, 2, 3, 3, 4.

Démonstration. Les caractères de $\mathfrak{S}_4$ donnent naturellement des caractères de $\tilde{\mathfrak{S}}_4$, via le morphisme de passage au quotient $\tilde{\mathfrak{S}}_4 \to \mathfrak{S}_4$. On les notera par la même lettre. On vérifie que l'on obtient pour l'instant les caractères suivants de $\tilde{\mathfrak{S}}_4$: χ_0, ε, χ, $\varepsilon\chi$, ϕ. Ils sont distincts sur $\mathfrak{S}_4$, donc sur $\tilde{\mathfrak{S}}_4$.

Les caractères χ_{std} et $\varepsilon\chi_{\text{std}}$ diffèrent en z : $\chi_{\text{std}}(z) = -2 \neq 2 = (\varepsilon\chi_{\text{std}})(z)$.

On obtient donc des représentations irréductibles de degrés 1, 1, 2, 2, 2, 3 et 3, soit déjà sept représentations parmi un nombre cherché entre 8 et 10. Calculons : $48 - (1^2 + 1^2 + 2^2 + 2^2 + 2^2 + 3^2 + 3^2) = 16$, nombre qui, par bonheur, est un carré, et qui ne s'écrit par ailleurs aucunement comme somme de deux ou de trois carrés non nuls.

Il en résulte qu'il y a huit caractères irréductibles et donc huit classes de conjugaison. Ainsi, chaque classe d'éléments d'ordre 2 de $\mathfrak{S}_4$ se relève en une seule classe. On notera donc $\tilde{2}_1$ (resp. $\tilde{2}_2$) la classe qui relève 2_1 (resp. 2_2).□

6.4. Calcul de la table des caractères de $\tilde{\mathfrak{S}}_4$

La stratégie pour trouver la table des caractères est maintenant directe. La table des caractères de $\mathfrak{S}_4$ nous donne directement les caractères χ_0, ε, χ, $\varepsilon\chi$, ϕ de $\tilde{\mathfrak{S}}_4$.

On détermine χ_{std} (et donc $\varepsilon\chi_{\text{std}}$, par le lemme 1.3) : les relèvements d'une rotation d'ordre fini et d'angle θ ont pour valeurs propres $\exp \pm i\theta/2$ pour l'un, $\exp \pm i(\theta/2 + \pi)$, pour l'autre, donc leurs traces sont $2\cos\theta/2$ et $-2\cos\theta/2$. Dans notre cas, les angles sont $\pm\pi$, $\pm 2\pi/3$ ou $\pm\pi/2$. On a donc, en déterminant la dernière ligne par orthogonalité des colonnes (voir

l'équation X-C.12) la table de caractères de $\tilde{\mathfrak{S}}_4$.

nom classe	1	z	$\tilde{2}_1$	$\tilde{3}$	$\tilde{\tilde{3}}$	$\tilde{4}$	$\tilde{4}'$	$\tilde{2}_2$
χ_0	1	1	1	1	1	1	1	1
ε	1	1	−1	1	1	−1	−1	1
χ	3	3	−1	0	0	1	1	−1
$\varepsilon\chi$	3	3	1	0	0	−1	−1	−1
ϕ	2	2	0	−1	−1	0	0	2
χ_{std}	2	−2	0	1	−1	$\sqrt{2}$	$-\sqrt{2}$	0
$\varepsilon\chi_{\text{std}}$	2	−2	0	1	−1	$-\sqrt{2}$	$\sqrt{2}$	0
ψ	4	−4	0	−1	1	0	0	0

6.5. Graphe de McKay de $\tilde{\mathfrak{S}}_4$

On procède donc comme pour les groupes binaires diédraux, c'est-à-dire que l'on prend le produit tensoriel d'un caractère avec χ_{std}, on le décompose et l'on recommence avec les nouveaux caractères obtenus, en utilisant la proposition 2.1. Plus précisément, si, à l'étape n, on obtient un caractère η avec η' dans la décomposition de $\eta\chi_{\text{std}}$, alors, à l'étape $n+1$, on calcule directement $\eta'\chi_{\text{std}} - \eta$, car on sait déjà, par symétrie, que η est dans la décomposition de $\eta'\chi_{\text{std}}$.

On va utiliser la symétrie du graphe : par la proposition 2.4, le groupe $\mathbb{Z}/2\mathbb{Z}$ agit sur le graphe par la multiplication d'un caractère par ε.

Les résultats suivants se calculent sans encombre :

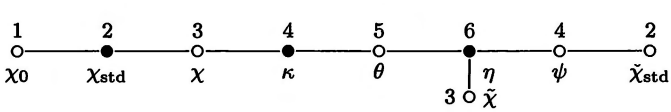
$$\chi_0\chi_{\text{std}} = \chi_{\text{std}},\ \chi_{\text{std}}\chi_{\text{std}} - \chi_0 = \chi,\ \chi\chi_{\text{std}} - \chi_{\text{std}} = \psi.$$

On sait donc que χ et ψ sont reliés par une arête du graphe et donc par symétrie, $\varepsilon\chi$ et $\varepsilon\psi = \psi$ le sont aussi. Il est donc judicieux de calculer $\psi\chi_{\text{std}} - \chi - \varepsilon\chi$, qui donne ϕ. Le reste du graphe s'obtient aisément par symétrie.

7. Groupe binaire icosaédral

Soit $\mathfrak{A}_5$ le groupe de symétries d'un icosaèdre et soit $\tilde{\mathfrak{A}}_5 = \varpi^{-1}(\mathfrak{A}_5)$ le *groupe binaire icosaédral.*

7.1. Proposition. *Le graphe de McKay du groupe binaire icosaédral est*[11] *:*



[11] Mêmes conventions que dans la proposition 4.1.

7.2. Degrés des caractères et nombre de classes de conjugaison

On a déjà vu au §X-2.1 la table des caractères de $\mathfrak{A}_5$. Rappelons-la pour mémoire.

nom classe	1	2	3	5_1	5_2
1	1	1	1	1	1
ψ	4	0	1	-1	-1
θ	5	1	-1	0	0
χ	3	-1	0	$\frac{\sqrt{5}+1}{2}$	$\frac{-\sqrt{5}+1}{2}$
$\check{\chi}$	3	-1	0	$\frac{-\sqrt{5}+1}{2}$	$\frac{\sqrt{5}+1}{2}$

7.3. Lemme. *Le groupe $\tilde{\mathfrak{A}}_5$ possède neuf classes de conjugaison :*

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
ordre	1	2	4	3	6	5	10	5	10
cardinal	1	1	30	20	20	12	12	12	12

Ses neuf caractères irréductibles ont pour degrés 1, 2, 2, 3, 3, 4, 4, 5, 6.

Les caractères de $\mathfrak{A}_5$ donnent naturellement des caractères de $\tilde{\mathfrak{A}}_5$, via le morphisme de passage au quotient $\tilde{\mathfrak{A}}_5 \to \mathfrak{A}_5$. On les notera idem.

Démonstration. On sait que $\tilde{\mathfrak{A}}_5$ possède neuf ou dix classes de conjugaison et autant de caractères irréductibles. On sait que parmi les degrés de caractères irréductibles, il y a ceux de $\mathfrak{A}_4$ et 2, degré de la représentation standard ($\tilde{\mathfrak{A}}_5$ est un sous-groupe de $\mathrm{SU}_2(\mathbb{C})$). Il s'agit donc de décomposer

$$120 - 1^2 - 3^2 - 3^2 - 4^2 - 5^2 - 2^2 = 56$$

comme une somme de trois ou quatre carrés. Il n'y a qu'une seule solution : $56 = 6^2 + 4^2 + 2^2$. D'où la liste des degrés irréductibles et le fait que $\tilde{\mathfrak{A}}_5$ a neuf classes de conjugaison : autrement dit, la classe des involutions de $\mathfrak{A}_5$ ne se scinde pas par relèvement dans $\tilde{\mathfrak{A}}_5$. □

7.4. Calcul de la table des caractères

On procède comme pour les groupes précédents, c'est-à-dire que l'on part du caractère trivial, on prend le produit tensoriel avec χ_{std}, on le décompose et l'on recommence. Mais, cette fois-ci, il n'y a pas d'action très intéressante de $\mathrm{Mor}(\tilde{\mathfrak{A}}_5, \mathbb{C}^*)$ sur le graphe de McKay. On a bien une action du groupe de Galois sur les caractères, mais celle-ci ne stabilise pas χ_{std}. On pouvait s'attendre au pire : $\mathbb{Z}/3\mathbb{Z}$ agit dans le cas E_6, $\mathbb{Z}/2\mathbb{Z}$ pour E_7, eh bien, ce sera[12] $\mathbb{Z}/1\mathbb{Z}$ pour E_8. Voici un résumé des résultats.

[12] Un collègue qui préfère rester dans l'anonymat nous fait remarquer qu'il s'agit là d'une preuve irréfutable que E_9 n'existe pas.

7.5. Proposition. *La table des caractères de* $\tilde{\mathfrak{A}}_5$ *est la suivante, avec* $\phi = \frac{\sqrt{5}+1}{2}$ *et* $\bar{\phi} = \frac{-\sqrt{5}+1}{2}$.

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
cardinal	1	1	30	20	20	12	12	12	12
χ_0	1	1	1	1	1	1	1	1	1
χ_{std}	2	−2	0	1	−1	$-\phi$	ϕ	$-\bar{\phi}$	$\bar{\phi}$
$\chi = \chi_{\text{std}}^2 - 1$	3	3	−1	0	0	ϕ	ϕ	$\bar{\phi}$	$\bar{\phi}$
$\kappa = \chi\chi_{\text{std}} - \chi_{\text{std}}$	4	−4	0	−1	1	−1	1	−1	1
$\theta = \kappa\chi_{\text{std}} - \chi$	5	5	1	−1	−1	0	0	0	0
$\eta = \theta\chi_{\text{std}} - \kappa$	6	−6	0	0	0	1	−1	1	−1
$\check{\chi} = \eta/\chi_{\text{std}}$	3	3	−1	0	0	$\bar{\phi}$	$\bar{\phi}$	ϕ	ϕ
$\psi = \eta\chi_{\text{std}} - \theta - \check{\chi}$	4	4	0	1	1	−1	−1	−1	−1
$\check{\chi}_{\text{std}} = \psi\chi_{\text{std}} - \eta$	2	−2	0	1	−1	$-\bar{\phi}$	$\bar{\phi}$	$-\phi$	ϕ

Démonstration. Voici les points principaux de la preuve, le détail des calculs étant laissé au lecteur. On calcule χ_{std} grâce au lemme 1.3 : la trace du relèvement dans $\mathrm{SU}_2(\mathbb{C})$ d'une rotation d'angle α est $\pm 2\cos\alpha/2$. Rappelons que les classes $\tilde{5}_1$ et $\widetilde{10}_1$ (resp. $\tilde{5}_2$ et $\widetilde{10}_2$) relèvent les rotations d'angle $2\pi/5$ (resp. $4\pi/5$), que $\cos(\pi/5) = (\sqrt{5}+1)/4 = \phi/2$ et que $\cos(2\pi/5) = (\sqrt{5}-1)/4 = -\bar{\phi}/2$.

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
χ_0	1	1	1	1	1	1	1	1	1
χ_{std}	2	−2	0	1	−1	$-\phi$	ϕ	$-\bar{\phi}$	$\bar{\phi}$

On sait que le caractère trivial apparaît dans χ_{std}^2 ; on calcule la différence.

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
cardinal	1	1	30	20	20	12	12	12	12
$\chi = \chi_{\text{std}}^2 - 1$	3	3	−1	0	0	ϕ	ϕ	$\bar{\phi}$	$\bar{\phi}$

On connaît déjà χ ; il est irréductible. On calcule ensuite $\chi\chi_{\text{std}} - \chi_{\text{std}}$.

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
cardinal	1	1	30	20	20	12	12	12	12
$\chi\chi_{\text{std}}$	6	−6	0	0	0	$-\phi-1$	$\phi+1$	$-\bar{\phi}-1$	$\bar{\phi}+1$
$\kappa = \chi\chi_{\text{std}} - \chi_{\text{std}}$	4	−4	0	−1	1	−1	1	−1	1

On vérifie que κ est irréductible : $\langle \kappa, \kappa \rangle = 1$. On calcule $\kappa\chi_{\text{std}}$, caractère où apparaît nécessairement χ, que l'on retranche.

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
cardinal	1	1	30	20	20	12	12	12	12
$\kappa\chi_{\text{std}}$	8	8	0	-1	-1	ϕ	ϕ	$\bar{\phi}$	$\bar{\phi}$
$\theta = \kappa\chi_{\text{std}} - \chi$	5	5	1	-1	-1	0	0	0	0

Le caractère θ est irréductible : $\langle \theta, \theta \rangle = 1$. On calcule $\theta\chi_{\text{std}}$ et l'on soustrait le caractère κ :

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
cardinal	1	1	30	20	20	12	12	12	12
$\theta\chi_{\text{std}}$	10	-10	0	-1	1	0	0	0	0
$\eta = \theta\chi_{\text{std}} - \kappa$	6	-6	0	0	0	1	-1	1	-1

Le caractère η est bien irréductible : $\langle \eta, \eta \rangle = 1$. On multiplie par χ_{std} pour obtenir un caractère de degré 12 dans lequel apparaît nécessairement θ :

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
cardinal	1	1	30	20	20	12	12	12	12
$\eta\chi_{\text{std}}$	12	12	0	0	0	$-\phi$	$-\phi$	$-\bar{\phi}$	$-\bar{\phi}$
$\eta\chi_{\text{std}} - \theta$	7	7	-1	1	1	$-\phi$	$-\phi$	$-\bar{\phi}$	$-\bar{\phi}$

Mais, ce caractère n'est pas irréductible : $\langle \eta\chi_{\text{std}} - \theta, \eta\chi_{\text{std}} - \theta \rangle = 2$. Les deux caractères qui le composent ne sont pas encore apparus, sauf éventuellement η. Mais si l'un des composants était η, l'autre serait de degré 1, ce qui est impossible car le seul caractère de degré 1 est χ_0, que l'on a déjà vu. Par suite, $\eta\chi_{\text{std}} - \theta$ est la somme d'un caractère de degré 3 et d'un de degré 4. De plus, puisque l'on a : $\chi_{\text{std}}(z) = \eta(z) = -1$, il vient : $\chi_{\text{std}}\eta(z) = 1$. Autrement dit, les caractères cherchés sont des caractères de degrés 3 et 4 de $\mathfrak{A}_5$, qui ne sont pas encore apparus, à savoir : $\check{\chi}$ et ψ. Au passage, $\check{\chi}$ provient de χ par action du groupe de Galois de $\mathrm{Gal}\big(\mathbb{Q}(\sqrt{5})/\mathbb{Q}\big)$. Et l'on vérifie que $\check{\chi}\chi_{\text{std}} = \eta$, de sorte que le sommet $\check{\chi}$ n'est relié qu'à η.

On vérifie par acquit de conscience que l'on a bien : $\eta\chi_{\text{std}} = \theta + \check{\chi} + \psi$:

nom classe	1	z	$\tilde{4}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}_1$	$\widetilde{10}_1$	$\tilde{5}_2$	$\widetilde{10}_2$
cardinal	1	1	30	20	20	12	12	12	12
$\eta\chi_{\text{std}} - \theta$	7	7	-1	1	1	$-\phi$	$-\phi$	$-\bar{\phi}$	$-\bar{\phi}$
$\psi = \eta\chi_{\text{std}} - \theta - \check{\chi}$	4	4	0	1	1	-1	-1	-1	-1

On calcule le produit $\psi\chi_{\mathrm{std}}$, duquel on retranche η.

nom classe cardinal	1 1	z 1	$\tilde{4}$ 30	$\tilde{3}$ 20	$\tilde{6}$ 20	$\tilde{5}_1$ 12	$\widetilde{10}_1$ 12	$\tilde{5}_2$ 12	$\widetilde{10}_2$ 12
$\psi\chi_{\mathrm{std}}$	8	-8	0	1	-1	ϕ	$-\phi$	$\bar{\phi}$	$-\bar{\phi}$
$\check{\chi}_{\mathrm{std}} = \psi\chi_{\mathrm{std}} - \eta$	2	-2	0	1	-1	$-\bar{\phi}$	$\bar{\phi}$	$-\phi$	ϕ

On voit à nouveau que $\check{\chi}_{\mathrm{std}}$ s'obtient à partir de χ_{std} en renumérotant les classes d'éléments d'ordre 5 de $\mathfrak{A}_5$ ou par action d'un groupe de Galois ($\sqrt{5} \leftrightarrow -\sqrt{5}$, ou $\phi \leftrightarrow \bar{\phi}$), voir exercice X-F.23. La table des caractères est complète. □

8. Versant géométrique de la correspondance

Deux séries infinies, trois groupes exceptionnels, une « recette » à base de produit tensoriel pour associer un graphe $\tilde{\Gamma}$ à un sous-groupe fini[13] G de $\mathrm{SU}_2(\mathbb{C})$. Qu'y a-t-il de si étonnant là-dedans ? Si l'article de John McKay a fait sensation, c'est que ce n'était pas la première correspondance entre ces sous-groupes et ces diagrammes qu'il venait de mettre à jour. Dès 1934, Patrick Du Val [23] en avait déjà établi une première en étudiant la géométrie du quotient $X = \mathbb{C}^2/G$.

8.1. Graphe associé à la désingularisation de $\mathbb{C}^2/G$: résumé

Comme G n'agit pas librement sur $\mathbb{C}^2$, il ne faut pas s'attendre à ce que la variété (algébrique) X soit lisse : l'image de 0 par la projection $\mathbb{C}^2 \to \mathbb{C}^2/G$ est un point singulier. On peut prouver qu'il existe une désingularisation canonique de X, c'est-à-dire une variété lisse $\tilde{X}$ et un morphisme $\pi : \tilde{X} \to X$ qui, par restriction, donne un isomorphisme de $\tilde{X} \setminus \pi^{-1}(0)$ sur $X \setminus \{0\}$. On travaille sur le diagramme suivant :

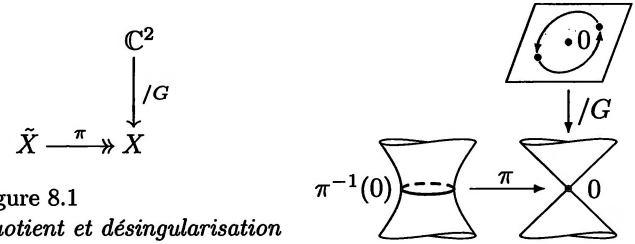


Figure 8.1
Quotient et désingularisation
Cas de $G = \mathbb{Z}/2\mathbb{Z}$

[13] Noter le subtil glissement de notation : dans cette partie, nous ne considérons plus qu'un seul groupe et nous abandonnons le « tilde » sur le nom du groupe.

La fibre singulière, c'est-à-dire $\pi^{-1}(0)$, est une réunion de courbes isomorphes à $\mathbb{P}^1$. On définit un graphe Γ : ses sommets sont les courbes précédentes ; on met une arête entre deux sommets si les courbes correspondantes se coupent.

La correspondance entre les résultats de Du Val et de McKay est la suivante : *le graphe Γ est le sous-graphe de $\tilde{\Gamma}$ obtenu en supprimant le sommet de $\tilde{\Gamma}$ associé à la représentation triviale.*

Il est un peu mystérieux que la courbe X retienne une bonne partie des informations concernant le groupe G et ses représentations alors que l'on a quotienté par le groupe. En termes imagés, la géométrie du quotient « voit » toujours le groupe !

Le mystère a été expliqué conceptuellement en 1983 grâce à Gérard Gonzalez-Sprinberg et Jean-Louis Verdier, voir [37]. Ils ont mis en dualité des invariants de la surface $\mathbb{C}^2/G$ d'une part, de la surface $\mathbb{C}^2$ munie de l'action de G d'autre part. Dans ces derniers, appelés *groupes de K-théorie (équivariante)*, on retrouve naturellement une trace des composantes irréductibles de $\pi^{-1}(0)$ et des caractères de G. Cette dualité a été réinterprétée en 1991 par Mikhail Kapranov et Éric Vasserot dans [44], avec un cadre conceptuel plus large appelé *dualité de Koszul*.

Mais ce n'est pas la fin de l'histoire ! Il faudrait étendre à des groupes plus gros que $\mathrm{SU}_2(\mathbb{C})$, parler de schémas de Hilbert pour réaliser des désingularisations, de *flips* et de *flops*, de groupes de réflexions symplectiques, c'est la boîte de Pandore que nous avons ouverte et nous voilà bien enzutés !

La fin de cette partie est une esquisse de la construction de $\tilde{X}$ et du graphe Γ évoqué ci-dessus lorsque G est un groupe cyclique. Il s'agit de faire subir un certain nombre d'éclatements à X et d'observer la fibre singulière.

8.2. Désingularisation de $\mathbb{C}^2/G$ avec G cyclique

Fonctions sur le quotient et invariants

Ici, on fixe un entier $n \geqslant 2$, une racine primitive n-ième de l'unité ζ et l'on note :

$$G = \left\{ \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix},\ k \in \mathbb{Z} \right\};\quad \zeta^n = 1.$$

On note (x_1, x_2) la base duale de la base canonique de $\mathbb{C}^2$, si bien que l'algèbre des fonctions polynomiales sur $\mathbb{C}^2$ s'identifie à l'algèbre de polynômes $\mathbb{C}[x_1, x_2]$. On hérite[14] d'une action linéaire de G sur $\mathbb{C}[x_1, x_2]$: pour g de G et P de $\mathbb{C}[x_1, x_2]$, on pose $g \cdot P = P \circ g^{-1}$.

[14] Il revient au même d'étendre l'action de G de $E = \mathbb{C}x_1 \oplus \mathbb{C}x_2$ à $\mathscr{S}(E) = \mathbb{C}[x_1, x_2]$ comme dans l'exercice X-F.38.

On note $\mathbb{C}[x_1, x_2]^G$ l'algèbre des invariants. Il est naturel de considérer cette algèbre comme l'algèbre des fonctions polynomiales sur le quotient $\mathbb{C}^2/G$. (Une fonction sur le quotient, c'est une fonction sur les représentants qui est invariante par le groupe. En oubliant le caractère polynomial, voir la preuve de la proposition X-B.15 (i).)

8.3. Proposition. *Soit $n \in \mathbb{N}^*$ et soit $G = \mathbb{Z}/n\mathbb{Z}$ agissant par homothéties sur $\mathbb{C}^2$. On a :*

$$\mathbb{C}[x_1, x_2]^G = \mathbb{C}[x_1^n, x_2^n, x_1 x_2] \simeq \mathbb{C}[x, y, z]/(xy - z^n).$$

Démonstration. C'est l'exercice X-F.44, qui utilise les séries de Molien. □

Cette écriture présente le quotient $\mathbb{C}^2/G$ comme la surface X_n de $\mathbb{C}^3$ (coordonnées (x, y, z)) définie par l'équation $z^n = xy$. Cette surface possède une singularité isolée à l'origine. Il s'agit de donner une résolution plus ou moins explicite de cette singularité. Pour cela, on utilise la notion d'éclatement vaguement présentée dans l'annexe B.

Éclatement de X_n (principe)

On reprend les notations du §B.5. L'éclatement B_n de X_n à l'origine O est l'adhérence de $p^{-1}(X_n \setminus \{O\})$ dans $\mathbb{B}$.

D'abord, on écrit des équations de $p^{-1}(X_n)$ dans les ouverts affines U_x, U_y et U_z (où U_x est défini par $x' \neq 0$, etc.). L'idée est de remplacer, dans $z^{n-2}z^2 - xy = 0$, les monômes z^2, x et y par des variables primées.

Dans U_x, l'intersection $p^{-1}(X_n) \cap U_x$ est décrite par :

$$p^{-1}(X_n)\cap U_x : \begin{cases} y = \dfrac{xy'}{x'},\ z = \dfrac{xz'}{x'},\ yz' = zy', \\ z^{n-2}\dfrac{x^2 z'^2}{x'^2} - \dfrac{x^2 y'}{x'} = 0; \end{cases} \Leftrightarrow \begin{cases} y = \dfrac{xy'}{x'},\ z = \dfrac{xz'}{x'}, \\ x^2(z^{n-2}z'^2 - x'y') = 0. \end{cases}$$

On trouverait de même, $p^{-1}(X_n)\cap U_y$ en remplaçant x par y et inversement. Pour ce qui est de $p^{-1}(X_n) \cap U_z$, on écrit :

$$p^{-1}(X_n)\cap U_z : \begin{cases} x = \dfrac{zx'}{z'},\ y = \dfrac{zy'}{z'},\ xy' = yx', \\ z^n - \dfrac{z^2 x' y'}{z'^2} = 0; \end{cases} \Leftrightarrow \begin{cases} x = \dfrac{zx'}{z'},\ y = \dfrac{zy'}{z'}, \\ z^2(z^{n-2}z'^2 - x'y') = 0. \end{cases}$$

Cherchons maintenant des équations de B_n. Plus précisément, montrons qu'elles s'obtiennent en supprimant des équations ci-dessus les facteurs x^2, y^2 et z^2.

Observons que pour $(x,y,z) \in X_n \cap U_x$, si $x=0$, alors $xy' = yx'$ et $x' \neq 0$ forcent $y=0$; on obtient de même $z=0$. Ainsi, il n'existe pas de point dans $p^{-1}(X_n \setminus \{O\}) \cap U_x$ tel que $x=0$. Il en est de même avec y et z.

Ainsi, les équations de l'adhérence de $p^{-1}(X_n \setminus \{O\}) \subset \mathbb{C}^3 \times \mathbb{P}^2$ sont :

$$B_n : \begin{cases} xy'=yx',\ xz'=zx',\ yz'=zy' \\ z^{n-2}z'^2 - x'y' = 0. \end{cases}$$

Éclatement de X_2

Pour $n=2$, on voit ainsi que B_2 est la sous-variété de $\mathbb{B}$ définie par l'équation homogène $z'^2 = x'y'$. Bien que ce soit la même équation que celle de X_2, vu que $[x' : y' : z']$ est un point de $\mathbb{P}^2$ et non de $\mathbb{C}^3$, B_2 est *lisse*. (Concrètement, le point singulier serait $[0,0,0]$...)

Ainsi, avec un éclatement, on rend X_2 lisse. On observe également que la fibre au-dessus de $O \in X_2$ est la conique d'équation $z'^2 = x'y'$ dans $\mathbb{P}^2$: elle est isomorphe à $\mathbb{P}^1$. Voir ci-dessus la figure 8.1.

Éclatement de X_3

Posons maintenant $n=3$. La sous-variété B_3 de $\mathbb{B}$ définie par l'équation $zz'^2 = x'y'$ est encore lisse (calculer le gradient !). La fibre au-dessus de O est la réunion des deux $\mathbb{P}^1$ d'équations $x'=0$ et $y'=0$, qui s'intersectent transversalement. Ainsi, le graphe des composantes du diviseur exceptionnel de la désingularisation de X_3 est A_2.

Éclatements de X_n (récurrence)

Pour $n \geqslant 4$, la sous-variété B_n de $\mathbb{B}$ définie par l'équation $z^{n-2}z'^2 = x'y'$ possède une singularité isolée : $\big((0,0,0),[0:0:1]\big)$. On peut regarder cette singularité dans l'ouvert U_z, dans lequel on peut fixer $z'=1$. On trouve alors l'équation

$$z^{n-2} = x'y'.$$

Ainsi, pour $n \geqslant 4$, B_n n'est plus lisse. L'éclatement a quand même un peu régularisé les choses, puisque la singularité est la même que celle de X_{n-2}. La fibre exceptionnelle de $B_n \to X_n$ est constituée des deux $\mathbb{P}^1$ d'équations $x'=0$ et $y'=0$, qui intersecteront transversalement le lieu exceptionnel après un nouvel éclatement (mais alors, ils ne s'intersecteront plus).

Cela permet de se convaincre que $\lfloor n/2 \rfloor$ éclatements permettent de résoudre X_n, et que le graphe des composantes irréductibles du diviseur exceptionnel de la résolution $Y_n \to X_n$ est le diagramme de Dynkin A_{n-1} : au premier éclatement, on fait apparaître les deux sommets extrêmes, et l'on se ramène à la singularité X_{n-2}.

Référence. Pour les autres sous-groupes, consulter par exemple [78, §6.1].

9. Une ubiquité remarquable

Le blog de John Baez[15] contient une introduction par John McKay lui-même à sa correspondance : `http://math.ucr.edu/home/baez/ADE.html`.

On vient de voir comment associer à chaque sous-groupe fini de $\mathrm{SU}_2(\mathbb{C})$ un graphe. La liste des graphes obtenus est :

$$\tilde{A}_n \ (n \geqslant 1),\ \tilde{D}_n \ (n \geqslant 4),\ \tilde{E}_6,\ \tilde{E}_7,\ \tilde{E}_8.$$

Pour chaque graphe, un sommet joue un rôle particulier : celui qui est associé à la représentation triviale. Quand on le supprime, on obtient la liste des diagrammes de Dynkin :

$$A_{n-1} \ (n \geqslant 1),\ D_{n+2} \ (n \geqslant 2),\ E_6,\ E_7,\ E_8.$$

L'ubiquité de ces graphes est spectaculaire.

9.1. Diagrammes de Dynkin et formes quadratiques

On a déjà rencontré ces diagrammes en cherchant les carquois qui n'ont qu'un nombre fini de représentations indécomposables. Étant donné un graphe (non orienté, fini) Γ ayant pour ensemble de sommets Γ_0 et pour ensemble d'arêtes Γ_1, on lui associe, comme dans le §III-7.1, sa *forme de Tits*, la forme quadratique q_Γ de la façon suivante :

- l'espace vectoriel sur lequel q_Γ est défini est $\mathbb{R}^{\Gamma_0}$;
- pour $x = (x_i)_{i\in\Gamma_0}$ dans $\mathbb{R}^{\Gamma_0}$, on pose :

$$q_\Gamma(x) = \sum_{i\in\Gamma_0} x_i^2 - \sum_{a:i-j} x_i x_j,$$

où la somme $\sum_{a:i-j}$ porte sur l'ensemble Γ_1 des arêtes (on note i et j les extrémités d'une arête a).

On rappelle le théorème III-B.2.

9.2. Théorème. *Soit Γ un graphe connexe. Alors, la forme quadratique q_Γ est définie positive si et seulement si Γ est un diagramme de Dynkin A_n $(n \geqslant 1)$, D_n $(n \geqslant 4)$, E_6, E_7 ou E_8.*

9.3. Remarques. (1) Si Γ n'est pas connexe, la forme q_Γ est somme directe des formes correspondant aux composantes.

(2) On vérifie immédiatement que tout sous-graphe connexe d'un graphe de Dynkin est un graphe de Dynkin.

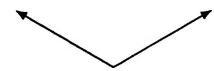
(3) Suivant John Baez[16], on peut reformuler le théorème de la façon suivante. Étant donné un graphe Γ, on veut associer à chaque sommet un

[15] La rumeur affirme que c'est le cousin de la chanteuse Joan.

[16] Voir son blog : `http://math.ucr.edu/home/baez/week230.html` ; voir aussi `http://math.ucr.edu/home/baez/week65.html`.

vecteur non nul dans un espace euclidien de sorte que deux vecteurs associés aux sommets d'une arête fassent entre eux un angle de 120°. C'est possible exactement lorsque Γ est une réunion disjointe de diagrammes de Dynkin. En effet, la restriction de la forme quadratique q_Γ au sous-espace engendré par deux vecteurs de base a pour matrice

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix}$$



ce qui décrit deux vecteurs de norme 1 faisant un angle de 120°.

Voici une preuve alternative au cas par cas du fait que tout diagramme de Dynkin correspond à une forme de Tits définie positive.

9.4. Lemme. *Si Γ est un diagramme de Dynkin, q_Γ est définie positive.*

Démonstration. Il suffit d'exhiber une famille libre $(\alpha_i)_{i\in\Gamma_0}$ dans un espace euclidien convenable E, de sorte que la matrice du produit scalaire euclidien (restreint à l'espace engendré par les α_i) soit la matrice de q_Γ. Pour d entier, on note $(\varepsilon_i)_{1\leqslant i\leqslant d}$ la base canonique de $\mathbb{R}^d$ euclidien standard.

- Si $\Gamma = A_n$, on prend $E = \mathbb{R}^{n+1}$ et l'on pose $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$ pour $1 \leqslant i \leqslant n$.
- Si $\Gamma = D_n$, on prend $E = \mathbb{R}^{n+1}$ et l'on pose $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$ pour $1 \leqslant i \leqslant n$ et $\alpha_n = \varepsilon_n + \varepsilon_{n+1}$.
- Si $\Gamma = E_8$, on prend $E = \mathbb{R}^8$ et l'on pose $2\alpha_1 = \varepsilon_1 + \varepsilon_8 + \sum_{2\leqslant i\leqslant 7} \varepsilon_i$, $\alpha_2 = \varepsilon_1 + \varepsilon_2$, $\alpha_i = \varepsilon_{i-1} - \varepsilon_{i-2}$ pour $3 \leqslant i \leqslant 8$.
- Si $\Gamma = E_7$ (resp. $\Gamma = E_6$), q_Γ s'identifie à la restriction de q_{E_8} au sous-espace engendré par $(\alpha_1, \ldots, \alpha_7)$ (resp. $(\alpha_1, \ldots, \alpha_6)$), et elle est donc définie positive.

Il semble peu naturel d'inventer ces familles de vecteurs, mais il est facile de vérifier que les produits scalaires sont corrects, ce qui au moins prouve le lemme. Pour plus d'explications sur la forme q_Γ, l'ouvrage de référence est le livre [10]. □

9.5. Lemme.

(i) *Soit Γ un graphe sans boucle (pas d'arête reliant un sommet à lui-même) admettant une fonction additive des sommets, c'est-à-dire qu'il existe $\mathbf{n} = (n_i)_{i\in\Gamma_0} \in (\mathbb{N}^*)^\Gamma$ telle que :*

$$\forall i \in \Gamma_0, \qquad 2n_i = \sum_{j-i} n_j.$$

Alors, $\mathbf{n}$ appartient au noyau de la forme q_Γ.

(ii) *Les graphes $\tilde{A}_n$ ($n \geqslant 0$), $\tilde{D}_n$ ($n \geqslant 4$), $\tilde{E}_6$, $\tilde{E}_7$, $\tilde{E}_8$ admettent des fonctions additives.*

9.6. Remarque. On peut montrer que les graphes de l'assertion (ii) sont les seuls graphes qui admettent une fonction additive, ce qui en donne une autre caractérisation élémentaire. Voir [6, Theorem 4.5.8].

Démonstration (*du lemme*). (i) On ne perd rien à supposer que $\Gamma_0=\{1,\dots,s\}$. Soit A la matrice d'adjacence du graphe Γ, c'est un élément de $\mathscr{M}_s(\mathbb{N})$. La matrice de q_Γ est $2\mathrm{I}_s-A$ et l'hypothèse traduit exactement que $\mathbf{n}$ appartient au noyau de $2\mathrm{I}_s - A$.

Écrivons la même chose avec des sommes. Soit B la forme bilinéaire symétrique associée à q_Γ. Comme une arête relie deux sommets, pour $x \in \mathbb{R}^{\Gamma_0}$, on a[17] :

$$B(\mathbf{n},x) = \sum_{i\in\Gamma_0}\Big(n_i x_i + \frac{1}{2}\sum_{j-i} n_j x_i\Big) = 0,$$

la dernière égalité provenant de l'hypothèse d'additivité. D'où l'assertion (i).

Soit $\tilde{\Gamma}$ un graphe apparaissant dans l'assertion (ii). Comme on a déjà rencontré $\tilde{\Gamma}$, l'existence d'une fonction additive n'est pas une surprise. On a vu comment associer à chaque sommet i de $\tilde{\Gamma}$ un caractère simple χ_i d'un sous-groupe G de $\mathrm{SU}_2(\mathbb{C})$. On a alors : $\chi_i\chi_{\mathrm{std}} = \sum_{j-i}\chi_j$. Évaluons en le neutre e de G et posons : $n_i = \chi_i(e)$. Alors, $(n_i)_{i\in\tilde{\Gamma}_0}$ est une fonction additive. On peut oublier le groupe... □

Démonstration (*du théorème*). Si Γ' est un sous-graphe de Γ et que $q_{\Gamma'}$ n'est pas définie positive, alors q_Γ non plus. Soit Γ un graphe tel que q_Γ est définie positive.

Le graphe Γ ne contient pas de boucle (*i.e.* d'arête reliant un sommet à lui-même), car la forme associée au graphe formé par un sommet et d boucles est $(1-d)x^2$, qui n'est pas définie positive.

Le graphe Γ ne contient pas de cycle (*i.e.* de sous-graphe isomorphe à $\tilde{A}_d$) ; sinon, il contient un sous-graphe isomorphe à $\tilde{A}_d$, qui admet une fonction additive.

Le nombre maximal d'arêtes issues d'un sommet de Γ (sa valence) est 3, car sinon, il contient un sous-graphe isomorphe à $\tilde{D}_4$, qui admet une fonction additive.

Le graphe Γ contient au plus un sommet de valence supérieure ou égale à 3 (un embranchement) ; sinon, il contient un sous-graphe isomorphe à $\tilde{D}_n$ pour $n \geqslant 5$, qui admet une fonction additive.

Si Γ n'a pas d'embranchement, il est donc de type A_n.

Sinon, c'est un arbre $Y_{p,q,r}$ ayant une racine d'où sont issues trois branches de longueurs p, q et r. Par exemple, D_5 s'identifie à $Y_{2,1,1}$. On supposera que $p \geqslant q \geqslant r$.

[17] À quelque(s) erreur(s) près, sans doute.

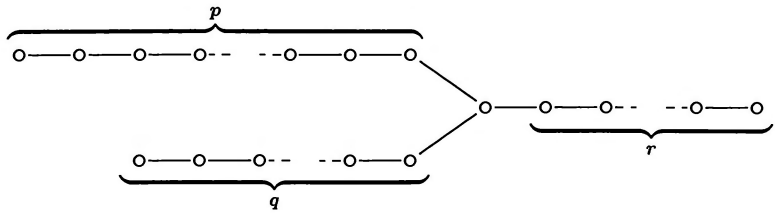


Figure 9.1. *Le graphe* $Y_{p,q,r}$

On a : $r = 1$, car sinon, Γ contient un sous-graphe isomorphe à $\tilde{E}_6$, qui admet une fonction additive.

On a : $q \leqslant 2$, car sinon, Γ contient un sous-graphe isomorphe à $\tilde{E}_7$, qui admet une fonction additive.

Si $q = 1$, Γ est de type D.

Enfin, si $q = 2$, on a : $r \leqslant 4$, car sinon, Γ contient un sous-graphe isomorphe à $\tilde{E}_8$, qui admet une fonction additive. Alors, Γ est de type E. □

9.7. Des diagrammes de Dynkin oubliés ?

Le lecteur qui a des lettres se demande sans doute pourquoi les séries sont appelées A_n, D_n et E_n. C'est qu'il faudrait ajouter deux séries infinies, B_n et C_n ($n \geqslant 2$) et deux diagrammes exceptionnels, F_4 et G_2 : voir la figure 9.2. Il ne s'agit plus exactement de graphes mais de *graphes valués* : une flèche double ⟹ (resp. triple ⟸) signifie que l'arête porte un *poids* $(2,1)$ (resp. $(3,1)$).

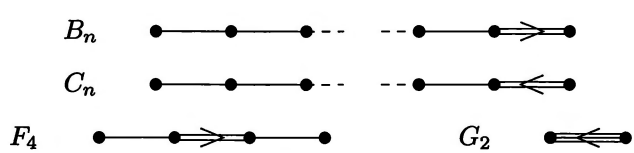


Figure 9.2. *Diagrammes de Dynkin* non simplement lacés

9.8. Autres occurrences des diagrammes de Dynkin

Outre ceux que nous avons déjà rencontrés, de nombreux problèmes de classification conduisent aux diagrammes de Dynkin :

- les groupes de Lie simples complexes : A_n correspond à $\mathrm{PSL}_n(\mathbb{C})$, B_n correspond à $\mathrm{PSO}_{2n+1}(\mathbb{C})$, C_n à $\mathrm{Sp}_{2n}(\mathbb{C})$, D_n à $\mathrm{PSO}_{2n}(\mathbb{C})$; les groupes E_n, E_7, E_8, F_4 et G_2 ne sont pas « classiques » ; voir [31, Chapter 23] ;
- les groupes de Lie compacts simples : A_n correspond à $\mathrm{U}_n(\mathbb{C})$, B_n correspond à $\mathrm{PSO}_{2n+1}(\mathbb{R})$, C_n à $\mathrm{Sp}(2n)$, D_n à $\mathrm{PSO}_{2n}(\mathbb{R})$; voir [31, Chapter 26] ;

- les carquois ayant un nombre fini de représentations indécomposables : il faut une définition étendue qui joue sur le corps de base pour prendre en compte les types B_n, C_n, F_4 et G_2 ; voir les *species* dans [6, Chapter 4] ;
- les sous-groupes finis d'un groupe orthogonal réel engendrés par des réflexions (on les appelle *groupes de réflexions*) : il faut alors ajouter quelques groupes oubliés comme $I_2(m)$ (le groupe diédral d'ordre $2m$), H_3 (le groupe de toutes les isométries d'un icosaèdre régulier) et H_4 (le groupe des isométries de la 600-cellule, *i.e.* l'enveloppe convexe du groupe $\tilde{\mathfrak{A}}_5$ dans $\mathrm{SU}_2(\mathbb{C}) \simeq \mathbf{S}^3$) ; voir [10] ;
- les sous-groupes finis de $\mathrm{SU}_2(\mathbb{C})$: la correspondance de McKay a été étendue par Peter Slodowy pour inclure les types B_n, C_n, F_4 et G_2 grâce à des paires de sous-groupes emboîtés remarquables ; voir [78, Appendix III] ;
- les *algèbres amassées* (connues comme *cluster algebras* en anglais) de dimension finie : introduites par Sergei Fomin et Andrei Zelevinsky au tournant du siècle, ces algèbres sont intensivement étudiées depuis, en lien avec de nombreux autres objets ; voir [85] ;
- etc.

10. John McKay : explorateur, découvreur de coïncidences, tisseur de liens...

Oh, I like that ! Such science and ego combined.
David Cronenberg, *Cosmopolis*, 2012.

John McKay est un mathématicien britannico-canadien, né en 1939. Bien sûr, il a classiquement démontré des théorèmes, par exemple la construction de certains groupes sporadiques[18]. Mais sa carrière est marquée par trois découvertes stupéfiantes, donnant lieu à d'incroyables développements. Au départ, une observation numérique simple établissant un lien entre deux objets apparemment très différents, comme on donnerait un coup de pioche sur l'orteil d'une statue enfouie dans le sable ; après McKay, des années de recherche pour dévoiler la statue.

Nous venons d'évoquer la correspondance McKay de 1979. En 1971, extrapolant sur des cas particuliers où il avait constaté cette coïncidence numérique, John McKay a émis la conjecture suivante : pour un groupe fini G, il y a autant de représentations irréductibles de dimension non divisible par 2 pour G que pour le normalisateur d'un de ses 2-Sylow (qui est, en général, un groupe bien plus petit que G). Réduire ainsi la théorie

[18] Les groupes finis simples se répartissent en vingt séries infinies, parmi lesquelles les groupes alternés $\mathfrak{A}_n$ ou les groupes $\mathrm{PSL}_n(\mathbb{F}_q)$, et vingt-six groupes qui ne font partie d'aucune série, appelés *sporadiques*. Cette classification est un des monuments les plus complexes des mathématiques.

des représentations du groupe à celle des normalisateurs des p-Sylow est un processus appelé *localisation*. La conjecture de McKay a été étendue par Jon Alperin pour d'autres nombres premiers que 2, puis affinée par Michel Broué dans certains cas particuliers (où « le groupe de défaut du bloc est abélien »...). C'est la source d'une quantité considérable de travaux difficiles sur la théorie des représentations des groupes finis.

Mais la plus spectaculaire des découvertes de McKay est sans doute le *monstrous moonshine*. Au départ, un constat :

$$196\,884 = 196\,883 + 1.$$

Et, là, stupeur ! D'une part, le nombre 196 884 est le premier coefficient significatif de ce que l'on appelle l'invariant modulaire[19] j : pour τ dans le demi-plan de Poincaré et $q = e^{i\pi\tau}$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + \dots$$

C'est une fonction méromorphe définie sur le demi-plan de Poincaré, invariante par le sous-groupe du groupe modulaire $\mathrm{PSL}_2(\mathbb{Z})$ (d'où son nom), et elle engendre toutes les autres. On en trouve une présentation dans le chapitre VII du *Cours d'arithmétique* de Jean-Pierre Serre [75].

D'autre part, 1 et 196 883 sont les dimensions des deux plus petites représentations irréductibles du monstre, le plus gros groupe sporadique (c'est-à-dire, un des vingt-six groupes finis simples qui ne font pas partie d'une famille infinie comme $\mathrm{PSL}_n(\mathbb{F}_q)$ ou $\mathrm{S}\Omega_n(\mathbb{F}_q)$).

En fait, McKay a vérifié que les premiers coefficients de j sont des sommes de dimensions de représentations du monstre. À partir de cette coïncidence numérique, McKay suggérait donc l'existence d'une relation entre deux objets que personne avant lui n'avait connectés, un invariant issu de la théorie des nombres d'un côté (j), un groupe fini exceptionnel de l'autre.

La relation a été établie par un détour en physique mathématique ! Richard Borcherds a terminé la construction d'un objet de structure très complexe, connu sous le nom d'algèbre d'opérateurs vertex, dont le groupe d'automorphisme est le monstre et qui est en particulier un espace vectoriel gradué $V = \bigoplus_{n \geqslant -1} V_n$ dont la série de Poincaré est : $\sum_{n \geqslant 1} q^n \dim V_n = j(\tau)$ (avec $q = e^{i\pi\tau}$). Chacun des espaces V_n est préservé par le monstre, ce qui explique le *moonshine*.

Le terme de *moonshine* a été attribué à ce phénomène par John H. Conway. Richard Borcherds, qui a reçu la médaille Fields en 1992 pour ses travaux sur le sujet, l'explique dans [9] :

[19] Cet invariant n'est pas sans lien avec celui que nous avons rencontré en VII-1.8...

[...] "Moonshine" is not a poetic terms referring to light from the moon. It means foolish or crazy ideas. (Quatsch in German.) A typical example of its use is the following quotation from E. Rutherford (the discoverer of the nucleus of the atom) : "The energy produced by the breaking down of the atom is a very poor kind of thing. Anyone who expects a source of power from the transformations of these atoms is talking moonshine."[20]

[20] *Moonshine* n'est pas un terme poétique se rapportant à la lumière de la Lune. Il signifie sornettes ou idées folles. (*Quatsch* en allemand.) Pour un exemple typique de son usage, voici une citation d'Ernest Rutherford (qui a découvert le noyau de l'atome) : « L'énergie produite par la fission d'un atome est une chose dérisoire. Une personne qui espère faire des transformations de ces atomes une source d'énergie est en train de dire des sottises. » Traduction libre.

A. Annexe. Produits tensoriels

La présentation du produit tensoriel adoptée ici est minimaliste, voire sous-minimale. Elle est inspirée de [67, exercice II-7]. On trouvera plus d'informations dans [56], p. 105 et suivantes, ou dans [46, chapitre XVI].

A.1. Produit tensoriel de deux matrices

Soient n et p deux entiers naturels non nuls et soient A une matrice $n \times n$ et B une matrice $p \times p$, toutes deux à coefficients complexes. De façon *ad hoc*, on définit le *produit tensoriel* de A et B comme la matrice $np \times np$ décrite par blocs de la façon suivante :

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & & & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{pmatrix} \in \mathscr{M}_{np}(\mathbb{C}).$$

A.2. Lemme. *Soient n et p deux entiers naturels non nuls et soient A et A' deux matrices complexes $n \times n$, et B et B' deux matrices complexes $p \times p$.*

(i) *On a : $(A \otimes B)(A' \otimes B') = AA' \otimes BB'$ dans l'algèbre des matrices $np \times np$.*

(ii) *On a : $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B)$.*

Démonstration. (i) La vérification est immédiate en effectuant le produit par blocs de taille $p \times p$: en notant $A = (a_{ij})$ et $A' = (a'_{ij})$, le bloc d'indice (i,j) du produit $(A \otimes B)(A' \otimes B')$ est :

$$\sum_{k=1}^{n} a_{ij} a'_{kj} BB',$$

qui est bien le coefficient d'indice (i,j) de AA' multiplié par la matrice BB'.

(ii) Dans la définition ci-dessus du produit tensoriel de deux matrices, on observe que les coefficients diagonaux de $A \otimes B$ sont les $a_{ii}b_{kk}$, où i décrit $\{1,\dots,n\}$ et k décrit $\{1,\dots,p\}$. La formule de la trace en résulte. □

A.3. Produit tensoriel de deux caractères

Étant donnés deux caractères χ et χ' d'un groupe fini G, on considère leur produit $\chi\chi'$ comme le produit point par point de deux fonctions :

$$\chi\chi' : G \to \mathbb{C}, \quad g \mapsto \chi(g)\chi'(g).$$

On va montrer que c'est le caractère d'une représentation de G, définie de façon unique à isomorphisme près. De plus, si l'on fixe deux représentations V et V' de caractère respectif χ et χ', nous expliciterons une

représentation $V \otimes V'$ dont le caractère est $\chi\chi'$, voir l'exercice A.5. Cette représentation, appelée *produit tensoriel* de V par V', va être décrite de façon *ad hoc* mais l'on pourrait en donner une construction intrinsèque.

A.4. Proposition. *Soit G un groupe fini et soient χ et χ' deux caractères*[21] *de G. Alors, le produit $\chi\chi'$ est le caractère d'une représentation de G, uniquement déterminée à isomorphisme près.*

Démonstration. Soient E et E' les espaces des représentations correspondant à χ et χ' et soient $n = \chi(1)$ et $n' = \chi'(1)$ leurs degrés respectifs. Via le choix de bases, les représentations donnent deux morphismes $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ et $\rho' : G \to \mathrm{GL}_{n'}(\mathbb{C})$. On considère l'application :

$$\rho \otimes \rho' : G \longrightarrow \mathrm{GL}_{nn'}(\mathbb{C}), \quad g \longmapsto \rho(g) \otimes \rho'(g).$$

L'assertion (i) du lemme A.2 exprime que $\rho \otimes \rho'$ est bien un morphisme de groupes, c'est-à-dire que l'on a bien défini une représentation de G. L'assertion (ii) prouve que le caractère de cette représentation est le produit $\chi\chi'$:

$$\forall g \in G, \quad \mathrm{tr}(\rho \otimes \rho')(g) = \mathrm{tr}\big(\rho(g) \otimes \rho'(g)\big) = \mathrm{tr}\,\rho(g)\,\mathrm{tr}\,\rho'(g) = \chi(g)\chi'(g).$$

L'assertion sur l'unicité provient comme d'habitude de l'unicité, à isomorphisme près, de la représentation associée à un caractère, voir X-B.9. □

A.5. Exercice. *On peut comprendre l'effet d'un changement de base de façon explicite. Soient n et n' des entiers non nuls. Montrer que :*

1. *si P (resp. P') est une matrice de $\mathrm{GL}_n(\mathbb{C})$ (resp. $\mathrm{GL}_{n'}(\mathbb{C})$), alors $P \otimes P'$ est inversible dans $\mathrm{GL}_{nn'}(\mathbb{C})$ et son inverse est $P^{-1} \otimes P'^{-1}$;*
   pour cela, utiliser le lemme A.2 (i) ;
2. *si de plus $A \in \mathrm{GL}_n(\mathbb{C})$ et $A' \in \mathrm{GL}_{n'}(\mathbb{C})$, alors*
$$(P \otimes P')(A \otimes A')(P \otimes P')^{-1} = (PAP^{-1}) \otimes (P'A'P'^{-1}) ;$$
3. *enfin, que la représentation $\rho \otimes \rho'$ est définie par ρ et ρ' indépendamment du choix des bases.*

A.6. Remarques

1. Bien que la construction du produit tensoriel ci-dessus dépende du choix de bases de E et E', on constate que son caractère ne dépend que des caractères χ et χ' : par suite, à isomorphisme près, la représentation ne dépend que des représentations E et E'. (C'est assez satisfaisant puisque de toute façon, χ ne détermine E qu'à isomorphisme près.)

[21] Rappel : ici, caractère est pris dans le sens de « caractère d'une représentation ».

2. Voici une présentation intrinsèque mais tortueuse du produit tensoriel. Étant donnés deux représentations $\rho : G \to \mathrm{GL}(V)$ et $\rho : G \to \mathrm{GL}(V')$ sur des espaces vectoriels V et V', on sait faire du dual V^* une représentation : pour g de G et ℓ de V^*, on définit $g \cdot \ell$ par :

$$\forall v \in V, \quad (g \cdot \ell)(v) = \ell \circ \rho(g^{-1})(v).$$

De même, on sait faire de l'espace $\mathscr{L}(V, V')$ des applications linéaires de V dans V' une représentation : pour g de G et f de $\mathscr{L}(V, V')$, on définit

$$g \cdot f = \rho'(g) \circ f \circ \rho(g^{-1}).$$

On peut alors définir la représentation produit tensoriel de V et V' comme : $V \otimes V' = \mathscr{L}(V^*, V')$. Cette présentation n'est pas très satisfaisante car elle cache la symétrie entre V et V' : or, puisque $\chi\chi' = \chi'\chi$, les représentations $V \otimes V'$ et $V' \otimes V$ sont isomorphes.

3. Dans ce paragraphe, on pourrait sans inconvénient remplacer $\mathbb{C}$ par un sous-corps quelconque.

Puissances tensorielles d'une représentation fidèle

A.7. Définition. On appelle *puissance tensorielle* n-ième d'une représentation V, que l'on notera $V^{\otimes n}$, du groupe G, la représentation V tensorisée n fois par elle-même : on convient que $V^{\otimes 0}$ est la représentation triviale, que $V^{\otimes 1} = V$ et que $V^{\otimes(n+1)} = V^{\otimes n} \otimes V$ pour tout n.

Soit G un groupe fini et soit χ_0 le caractère d'une représentation V de G. D'après ce qui précède, les puissances χ_0^n ($n \in \mathbb{N}$) sont les caractères de représentations, de dimensions respectives $\chi_0(1)^n$, que l'on a définies à isomorphisme près. On les appelle *puissances tensorielles* de la représentation V. Par exemple, $\chi_0^0 = 1$ est le caractère de la représentation triviale.

La proposition suivante n'est pas logiquement indispensable, mais, convenablement reformulée, elle justifie la stratégie pour trouver la table des caractères des sous-groupes finis de $\mathrm{SU}_2(\mathbb{C})$ en utilisant les puissances tensorielles de la représentation naturelle de degré 2.

A.8. Proposition. *Soit G un groupe fini et soit V une représentation de G de caractère χ_0. On suppose V fidèle, c'est-à-dire que le noyau du morphisme de représentation $\rho_0 : G \to \mathrm{GL}(V)$ est trivial. Alors, tout caractère χ de G apparaît dans une puissance tensorielle $V^{\otimes n}$:*

$$\exists n \in \mathbb{N}, \quad \langle \chi, \chi_0^n \rangle > 0.$$

Démonstration. Rappelons que le caractère de $V^{\otimes n}$ est χ_0^n. Considérons la fonction génératrice des multiplicités de χ dans χ_0^n, c'est-à-dire :

$$f(t) = \sum_{n \geqslant 0} \langle \chi, \chi_0^n \rangle t^n \in \mathbb{C}[[t]].$$

Par définition, c'est :

$$f(t) = \frac{1}{|G|} \sum_{g \in G} \sum_{n \geqslant 0} \overline{\chi(g)} \chi_0(g)^n t^n = \frac{1}{|G|} \sum_{g \in G} \frac{\overline{\chi(g)}}{1 - \chi_0(g)t}.$$

Pour $g \in G$, le nombre complexe $\chi_0(g)$ est par définition la trace de $\rho_0(g)$, et donc est une somme de $\dim(V)$ racines de l'unité, d'où (voir par exemple l'exercice X-F.26) :

$$\chi_0(g) = \dim V \iff \rho_0(g) = \mathrm{Id}_V .$$

Vu que V est fidèle, cela signifie que g est le neutre e de G et, dans ce cas, $\chi_0(e) = \dim V$. Il en résulte que f possède un pôle simple en $1/\dim V$ dont le résidu est

$$\lim_{t \to 1/\dim V} (1 - t \dim V) f(t) = \frac{\chi(e)}{|G|}.$$

Par suite, f n'est pas la fonction nulle, si bien que l'un au moins des coefficients $\langle \chi, \chi_0^n \rangle$ est non nul, donc strictement positif, puisqu'il s'agit de la multiplicité de χ dans χ_0^n. □

B. Annexe. Éclatements

Pour d entier naturel non nul, soit $\mathbb{A}^d$ l'espace affine de dimension d sur $\mathbb{R}$ ou $\mathbb{C}$.

B.1. Préliminaire : éclatement du plan en un point

Ici, $d = 2$. On fixe un système de coordonnées (x, y) sur $\mathbb{A}^2$. Cela donne une origine 0 et un système de coordonnées homogènes sur $\mathbb{P}^1$: pour $(x', y') \neq (0, 0)$, on notera $[x', y']$ la droite reliant 0 et (x', y'). L'égalité $t = y'/x'$ identifie $\mathbb{P}^1$ à $\mathbb{R} \cup \{\infty\}$ ou à $\mathbb{C} \cup \{\infty\}$.

L'*éclatement* de $\mathbb{A}^2$ en l'origine 0 est la surface[22] $\mathbb{B}^2$ de $\mathbb{A}^2 \times \mathbb{P}^1$ définie par :

$$\mathbb{B}^2 = \Big\{ \big((x, y), [x' : y']\big) \in \mathbb{A}^2 \times \mathbb{P}^1,\ xy' = yx' \Big\}.$$

Dans l'ouvert $U_x = \{x' \neq 0\} = \{t \neq \infty\}$, dans lequel on a trois coordonnées (x, y, t), $E \cap U_x$ est le paraboloïde hyperbolique d'équation $y = tx$ (cf. figure B.1, ci-après).

[22] La lettre $\mathbb{B}$ veut rappeler l'initiale de *blowup*. Les équations ont un sens malgré l'indétermination portant sur (x', y'), car elles sont homogènes.

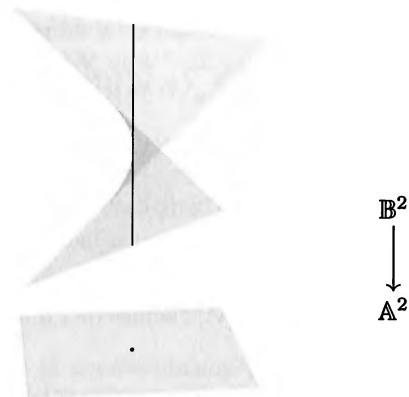


Figure B.1. *Éclatement du plan en un point*

La première projection $\mathbb{A}^2 \times \mathbb{P}^1 \to \mathbb{A}^2$ est un morphisme de variétés. On note p sa restriction à $\mathbb{B}^2$. Si $(x,y) \neq (0,0)$, on observe que $p^{-1}(x,y)$ est le singleton $\{((x,y),[x,y])\}$; en revanche, la fibre au-dessus de 0 est : $p^{-1}(0) = \{0\} \times \mathbb{P}^1$. Ainsi, p envoie toute la fibre $p^{-1}(0)$ sur 0 et établit une bijection du complémentaire $\mathbb{B} \setminus p^{-1}(0)$ sur $\mathbb{A}^2 \setminus \{0\}$. On a remplacé le plan $\mathbb{A}^2$ par une surface qui lui est très semblable où le point 0 a été remplacé par une droite projective : d'où le terme d'éclatement.

B.2. Éclatement d'une courbe en un point

Si X est une courbe de $\mathbb{A}^2$, son éclatement en 0 est la courbe définie par :

$$B = \overline{p^{-1}(X \setminus \{0\})}.$$

On note $\pi : \tilde{X} \to X$ la restriction de p à $\tilde{X}$. Vu les propriétés de p, la restriction de π à $B \setminus p^{-1}(0)$ est un isomorphisme vers $X \setminus \{0\}$. En pratique, si 0 est un point singulier de X, les points de $\pi^{-1}(0)$ sont « moins » singuliers que 0. On peut montrer qu'après un nombre fini d'éclatements, la courbe obtenue est lisse.

B.3. Exemples. Voici trois exemples simples (figure B.2).

1. Soit X la courbe d'équation $(x+y)y = 0$: c'est une réunion de deux droites sécantes. Restreignons-nous à l'ouvert affine $U_{x'}$, où l'on a trois coordonnées (x,y,t). On vérifie que l'intersection de B avec $U_{x'}$ est la réunion des deux droites non sécantes d'équations respectives $y + x = t + 1 = 0$ et $y = t = 0$. La fibre singulière $\pi^{-1}(0)$ est formée des deux points $(0,0,0)$ et $(0,0,-1)$.
2. Soit X la courbe d'équation $y^2 = x^3$. Pour un point (x,y) de X différent de l'origine, on a $x \neq 0$: on peut prendre pour coordonnée $t = y'/x'$.

On voit que :

$$p^{-1}(X \setminus \{0\}) = \{(x,y,t) \in \mathbb{A}^2 \times \mathbb{P}^1,\ x \neq 0 \text{ et } y^2 = x^3 \text{ et } t = y/x\}.$$

On voit que : $x^3 = y^2 = t^2x^2$ ce qui, avec $x \neq 0$, donne $x = t^2$, puis $y = t^3$. Passer à l'adhérence est très facile : B est la courbe paramétrée par $t \mapsto (t^2, t^3, t)$. En particulier, elle est lisse. La fibre singulière $\pi^{-1}(0)$ est réduite à un point.

3. Soit X la courbe d'équation $y^2 = x^2(x + 1/2)$. On a de même :

$$p^{-1}(X\setminus\{0\}) = \big\{(x,y,t) \in \mathbb{A}^2\times\mathbb{P}^1,\ x \neq 0 \text{ et } y^2 = x^2\big(x+\frac{1}{2}\big) \text{ et } t = y/x\big\}.$$

On voit que : $x^2(x + 1/2) = y^2 = t^2x^2$ ce qui, avec $x \neq 0$, donne $x = t^2 - 1/2$, puis $y = t^3 - t/2$. Ainsi, B est la courbe paramétrée par $t \mapsto (t^2 - 1/2, t^3 - t/2, t)$ — elle est lisse ! La fibre singulière $\pi^{-1}(0)$ est la paire $\{(0, 0, \pm 2^{-1/2})\}$.

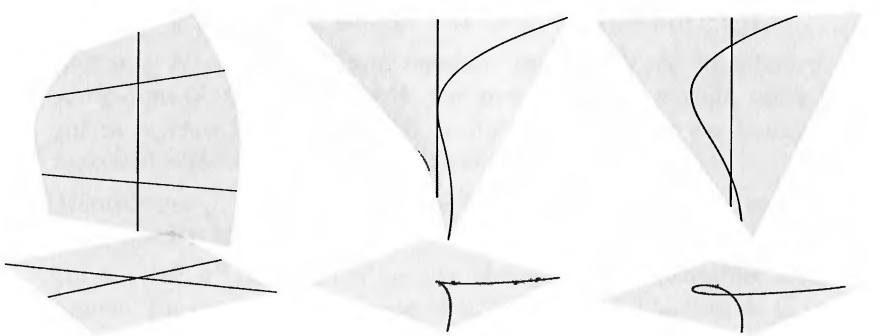


Figure B.2. *Trois exemples d'éclatements*

B.4. Remarque. La présentation de l'éclatement de X en 0 semble dépendre de l'injection de X dans $\mathbb{A}^2$ mais en fait, on peut le définir intrinsèquement. Pour ces questions, voir [64], p. 187 et suivantes.

B.5. Éclatement d'une surface dans l'espace en l'origine

On procède de même avec l'espace affine $\mathbb{A}^3$. On fixe des coordonnées (x, y, z) et des coordonnées homogènes $[x' : y' : z']$ sur $\mathbb{P}^2$. Alors, l'éclatement de l'origine est la sous-variété de $\mathbb{A}^3 \times \mathbb{P}^2$ suivante :

$$\mathbb{B} = \Big\{\big((x,y,z),[x' : y' : z']\big) \in \mathbb{A}^3 \times \mathbb{P}^2,\ xy' = yx',\ xz' = zx',\ yz' = zy'\Big\},$$

munie de la projection naturelle $p : \mathbb{B} \to \mathbb{A}^3$.

On voit que p est surjective, la fibre au-dessus d'un point $(x, y, z) \neq (0, 0, 0)$ est le point $\big((x, y, z), [x : y : z]\big)$, et la fibre au-dessus de $0 = (0, 0, 0)$ est le plan $\mathbb{P}^2 = \big\{(0, 0, 0)\big\} \times \mathbb{P}^2$.

Dans la suite, on désignera par U_x (resp. U_y, U_z) l'ouvert de $\mathbb{B}$ défini par $x' \neq 0$ (resp. $y' \neq 0$, $z' \neq 0$). Ces trois ouverts forment un recouvrement de $\mathbb{B}$.

Étant donnée une sous-variété X dans $\mathbb{A}^3$, l'éclatement de X en 0 est défini par :

$$B = \overline{p^{-1}(X) \setminus \{0\}}.$$

C. Exercices du chapitre XI

C.1. Exercice (Généralisation du graphe de McKay)

Soit G un groupe fini. On considère une famille finie de représentations complexes (irréductibles ou pas) $V_1, \dots, V_n$ et V une représentation isomorphe à sa duale. On note χ_i le caractère associé à V_i $(1 \leqslant i \leqslant n)$ et χ le caractère de V.

En s'inspirant de la preuve de la proposition 2.1, montrer que l'on a :

$$\langle \chi_i \otimes \chi, \chi_j \rangle_G = \langle \chi_j \otimes \chi, \chi_i \rangle_G.$$

On peut donc construire un graphe non orienté dont les sommets sont les V_i (pour $1 \leqslant i \leqslant n$) et où le nombre d'arêtes qui relient la paire $\{V_i, V_j\}$ est $\langle \chi_i \otimes \chi, \chi_j \rangle_G$.

C.2. Exercice (Action de G/H sur $\mathrm{Irr}(H)$)

Soit G un groupe fini et soit H un sous-groupe distingué de G. Pour tout $\pi \in \mathrm{Irr}(H)$ et g dans G, on pose $\pi^g : H \to \mathbb{C}$, $\pi^g(h) = \pi(g^{-1}hg)$.

1. *Soit $\rho : H \to \mathrm{GL}(W)$ une représentation de H de caractère π, et soit g dans G. On définit sur W une structure de H-module, notée W^g, par sa représentation associée $h \mapsto \rho(g^{-1}hg)$. Montrer que le caractère associé à cette nouvelle représentation est égal à π^g.*

2. *Montrer que $g \cdot \pi = \pi^g$ définit une action du groupe G/H (par isométries) sur $\mathrm{Irr}(H)$.*

   On a : $\langle \pi^g, \pi'^g \rangle_H = \langle \pi, \pi' \rangle_H$ par changement de variables dans la somme. En particulier, π^g reste bien irréductible. L'action de G passe au quotient par invariance de la trace.

3. *Soit V un G-module irréductible de caractère χ et soit V_H l'espace V muni d'une structure de H-module par restriction, de caractère $\chi|_H$. Soit W un sous-H-module irréductible de V_H, de caractère π. Montrer que $\langle \chi|_H, \pi^g \rangle_H = \langle \chi|_H, \pi \rangle_H$. En déduire que les irréductibles de $\mathrm{Irr}(H)$ dans une même G/H-orbite apparaissent avec la même multiplicité, que l'on notera m, dans la décomposition de $\chi|_H$.*

   Par invariance de la trace, on a : $(\chi|_H)^g = \chi|_H$ et donc :

   $$\langle \chi|_H, \pi^g \rangle_H = \langle (\chi|_H)^g, \pi^g \rangle_H = \langle \chi|_H, \pi \rangle_H,$$

   puisque G/H agit par isométries.

4. *Soit g dans G et soit $gW = \{g \cdot w,\ w \in W\}$ le sous-espace de V (bien défini puisque $W \subset V$ et G agit sur V). Montrer que $\sum_g gW = V$.*

   On a une inclusion et le membre de gauche est stable par G, d'où l'égalité par l'irréductibilité de V comme G-module.

5. *Montrer que V_H est une somme directe de gW.*
   Comme H est distingué, gW est bien un H-module, car h donné dans H, $hgW = g(g^{-1}hg)W \subset gW$. C'est bien sûr l'irréductibilité de W, et donc de gW, qui permet de conclure.
6. *On note I le stabilisateur dans G de π,* i.e. *le sous-groupe des k tels que $\pi^k = \pi$. Conclure que l'on a :*
$$\chi|_H = |I| \sum_{g \in R} \pi^g,$$
où g parcourt un ensemble R de représentants de G/I.

C.3. Exercice (Restriction dans le cadre des quotients abéliens)

Soit G un groupe fini et soit H un sous-groupe distingué de G tel que G/H soit abélien. Si l'on note p la projection canonique de G sur G/H, alors $\varepsilon \mapsto \varepsilon \circ p$ fournit un morphisme injectif du groupe abélien $(G/H)^* = \mathrm{Mor}(G/H, \mathbb{C}^*)$ dans $\mathrm{Mor}(G, \mathbb{C}^*)$. On identifiera l'image $A \subset \mathrm{Mor}(G, \mathbb{C}^*)$ de ce morphisme à $(G/H)^*$.

1. *On rappelle, voir exercice X-F.22, que le groupe $\mathrm{Mor}(G, \mathbb{C}^*)$ agit par produit tensoriel sur l'ensemble des caractères de G. Soient χ, χ' dans $\mathrm{Irr}(G)$; montrer que $\sum_{\varepsilon \in A} \langle \chi, \varepsilon \otimes \chi' \rangle_G = \langle \chi|_H, \chi'|_H \rangle_H$.*
   On pourra revenir à la définition du produit hermitien des caractères, puis regrouper les termes selon une décomposition $G = \bigcup_{g,h} gh$, où h parcourt H et g parcourt un système de représentants de G/H . Comme G/H est un groupe abélien, $\mathrm{Irr}(G/H) = (G/H)^* = A$ et la propriété d'orthogonalité des lignes de la table des caractères de G/H permet de simplifier largement le membre de gauche.
2. *Soit $I = I_\chi$ le stabilisateur dans A du caractère irréductible $\chi \in \mathrm{Irr}(G)$. Déduire de la formule précédente que*
$$\langle \chi|_H, \chi|_H \rangle_H = |A/I|.$$
   En déduire que l'orbite de χ est le singleton $\{A\}$ si et seulement si $\chi|_H$ reste irréductible.
3. *On suppose que G/H est d'ordre premier p et l'on considère $\pi \in \mathrm{Irr}(H)$ un caractère irréductible de la décomposition de $\chi|_H$. Pour tout g de G, soit π^g le caractère irréductible défini dans l'exercice C.2. Montrer que si la restriction de χ à H n'est pas irréductible, elle se scinde en somme de p caractères irréductibles distincts de la forme π^g.*
   Si la restriction n'est pas irréductible, alors $I \neq A$ et donc I est trivial. Donc, $\langle \chi|_H, \chi|_H \rangle_H = p$. D'après la question 6 de l'exercice C.2, il y a bien p irréductibles distincts sans multiplicité, et qui forment une orbite pour l'action de G/H.

Représentations induites

C.4. Exercice (Représentation induite ; généralités)

Soit G un groupe fini et soit H un sous-groupe de G. À partir d'une représentation W de H, on définit la représentation induite $\mathrm{Ind}_H^G(W)$ *(appelée aussi* coinduite *dans ce contexte) comme l'ensemble*

$$\mathrm{Ind}_H^G(W) = \big\{f : G \to W,\ f(hg) = h \cdot f(g), \forall g \in G,\ \forall h \in H\big\},$$

*muni de sa structure d'espace vectoriel naturel provenant de la structure d'espace de W et muni d'une action linéaire de G par $g \cdot f = f(?g)$ (*i.e. *$g \cdot f : h \mapsto f(hg)$).*

1. *Montrer que si $H = G$, alors les représentations W et $\mathrm{Ind}_H^G(W)$ sont naturellement isomorphes.*

   On montre que $w \mapsto f_w$, où $f_w : g \mapsto g \cdot w$, est un isomorphisme de représentations de G.

2. *À l'opposé, montrer que si $H = \{e\}$ et $W = \mathbb{C}_{\mathrm{triv}}$ est la représentation triviale, alors $\mathrm{Ind}_H^G(W)$ est isomorphe à la représentation régulière de G.*

   C'est fait dans la remarque X-C.2.

3. *Montrer que l'on a : $\dim \mathrm{Ind}_H^G(W) = [G : H] \dim W$.*

   Soient S un ensemble de représentants de $H\backslash G$ dans G et $(w_i)_{i\in I}$ une base de W, alors les fonctions f_{s,w_i} $(s \in S,\ i \in I)$ (bien) définies par $f_{s,w_i}(s') = \delta_{s,s'} w_i$, pour tout s' de S forment une base de $\mathrm{Ind}_H^G(W)$.

4. *On suppose que G est un sous-groupe de K. Montrer que la représentation induite $\mathrm{Ind}_G^K\big(\mathrm{Ind}_H^G(W)\big)$ est isomorphe à $\mathrm{Ind}_H^K(W)$.*

   À une fonction f de K dans $\mathrm{Ind}_H^G(W)$, on associera la fonction r de K dans W donnée par $r(k) = f(k)(1)$. Inversement, à une fonction r de K dans W, on associe la fonction f qui envoie k sur $f(k) : G \to W$ telle que $f(k)(g) = r(gk)$.

5. *Montrer que l'induit de H à G de la représentation régulière de H est la représentation régulière de G. En déduire que toute représentation irréductible de G est une sous-représentation de l'induite d'une représentation irréductible de H.*

La construction des représentations induites constitue un outil puissant pour fabriquer des représentations d'un groupe à partir des représentations de ses sous-groupes.

C.5. Exercice (Induction et représentation par permutation)

On veut montrer ici que la représentation par permutation définie au §X-B.14 est un cas particulier de représentation induite. Soit G un groupe fini agissant transitivement sur un ensemble X et soit $\mathbb{C}X$ la représentation associée

définie sur la base $(e_y)_{y\in X}$ *de* $\mathbb{C}X$ *par* $g\cdot e_y = e_{g\cdot y}$ *(*$g\in G$, $y\in X$*). On fixe un élément* x *dans* X *et l'on veut montrer que la représentation* $\mathbb{C}X$ *est isomorphe à* $\mathrm{Ind}_{G_x}^G(\mathbb{C}_{\mathrm{triv}})$*, où* G_x *est le stabilisateur de* x *et* $\mathbb{C}_{\mathrm{triv}}$ *la représentation triviale de* G_x*.*

1. *On fixe un système de représentants* S *pour les classes de* G/G_x*. Montrer que l'application*
$$f\in \mathrm{Ind}_{G_x}^G(\mathbb{C}_{\mathrm{triv}}) \longmapsto \Big(\sum_{g\in S} f(g^{-1})e_{g\cdot x}\Big)\in \mathbb{C}X$$
est un morphisme de représentations.
2. *Montrer que l'application qui envoie* $\sum_{y\in X}\alpha_y e_y$ *sur la fonction* f *définie par* $f(g)=\alpha_{g^{-1}\cdot x}$ *est le morphisme inverse.*
3. *Conclure :* $\mathrm{Ind}_{G_x}^G(\mathbb{C}_{\mathrm{triv}})\simeq \mathbb{C}X$*.*

C.6. Exercice (Caractère d'une représentation induite)

Soit G *un groupe fini et soit* $H\subset G$ *un sous-groupe. On veut calculer le caractère de la représentation induite d'une* H*-représentation* W *sur* G*. Comme dans l'exercice C.5, on note* S *un ensemble de représentants de* $H\backslash G$*, et pour tout* w *de* W *on désigne par* $f_{s,w}$ *l'élément de* $\mathrm{Ind}_H^G(W)$ *qui envoie* $s'\in S$ *sur* $\delta_{s,s'}w$*.*

1. *On note* W_s *le sous-espace de* $\mathrm{Ind}_H^G(W)$ *engendré par les* $f_{s,w}$*,* $w\in W$*. Montrer que* $\mathrm{Ind}_H^G(W)=\oplus_{s\in S}W_s$
2. *On fixe* g *dans* G*.*
   (a) *Montrer, en faisant agir* G *à droite sur l'ensemble des classes à gauche* $H\backslash G$*, que pour tout* s *dans* S*, il existe un unique* $s'\in S$*, et* h_s *dans* H *tels que* $sg^{-1}=h_s^{-1}s'$*.*
   (b) *Montrer que l'action de* g *sur* $f_{s,w}\in \mathrm{Ind}_H^G(W)$ *est donnée par* $g\cdot f_{s,w}=f_{s',h_s\cdot w}$*.*
   Il suffit de calculer $(g\cdot f_{s,w})(s'')$ pour $s''=s'$ et $s''\neq s'$.
   (c) *Montrer que l'action de* g *envoie* W_s *sur* $W_{s'}$ *et que si* $s'=s$*, alors la trace de* g*, considéré comme endomorphisme de* W_s*, est égale à* $\chi_W(h_s)$*, où* χ_W *désigne le caractère de* W*.*
   Si $s=s'$, alors g et h_s sont conjugués par s.
3. *Montrer que le caractère de la représentation induite est donné par*
$$\chi_{\mathrm{Ind}_H^G(W)}(g)=\sum_{\substack{s\in S\\ sgs^{-1}\in H}}\chi_W(sgs^{-1})=\frac{1}{|H|}\sum_{\substack{k\in G\\ kgk^{-1}\in H}}\chi_W(kgk^{-1}). \quad (\heartsuit)$$
   On calcule la trace de l'action de g par blocs en utilisant la question qui précède et la décomposition de $\mathrm{Ind}_H^G(W)$. La seconde égalité vient en changeant s en $k=h's$, $h'\in H$.

4. *Soit C_g la classe de conjugaison de g dans G. Le groupe H agit par conjugaison sur $C_g \cap H$ et l'on note $C_g \cap H = H_1 \cup \cdots \cup H_t$ sa décomposition en classes de conjugaison de H. Soit k_0 dans G tel que $k_0 g k_0^{-1}$ est dans H. Décrire l'ensemble des k de G tels que $kgk^{-1} = k_0 g k_0^{-1}$, puis, montrer que*

$$\chi_{\mathrm{Ind}_H^G(W)}(g) = \frac{1}{|H|} \sum_{h \in C_g \cap H} \chi_W(h) \frac{|G|}{|C_g|} = \frac{[G:H]}{|C_g|} \sum_{i=1}^{t} \chi_W(H_i)|H_i|,$$

où $\chi_W(H_i)$ désigne la valeur (constante) de χ_W sur la classe H_i.

5. *Montrer en particulier que pour la représentation triviale de H, on a :*

$$\chi_{\mathrm{Ind}_H^G(\mathbb{C}_{\mathrm{triv}})}(g) = \frac{[G:H]}{|C_g|} |C_g \cap H|.$$

C.7. Exercice (Induction et coloriages)

En utilisant l'exercice C.6, prouver la proposition V-5.36 sur le lien entre polynôme générateur des coloriages et induction.

Avec les notations de la proposition V-5.36, on a :

$$\frac{\chi_\rho(\lambda)}{z_\lambda} = \frac{[\mathfrak{S}_n : G]}{|C_\lambda| z_\lambda} |C_\lambda \cap G| = \frac{1}{|G|} |C_\lambda \cap G|,$$

car la classe de conjugaison C_λ de $\mathfrak{S}_n$ est de cardinal $|\mathfrak{S}_n|/z_\lambda$. On conclut par le corollaire V-5.20.

C.8. Exercice (Réciprocité de Frobenius)

Soit G un groupe fini d'élément neutre e et soit H un sous-groupe de G. Pour toute représentation W de H, on note $\mathrm{Ind}_H^G(W)$ la représentation induite sur G définie dans l'exercice C.4. Pour toute représentation V de G, on note $\mathrm{Res}_H^G(V)$ la restriction de V, c'est-à-dire l'espace V considéré comme représentation de H.

On va identifier $\mathrm{Hom}_G\big(V, \mathrm{Ind}_H^G(W)\big)$ et $\mathrm{Hom}_H\big(\mathrm{Res}_H^G(V), W\big)$.

1. *On veut définir $\Phi : \mathrm{Hom}_G\big(V, \mathrm{Ind}_H^G(W)\big) \to \mathrm{Hom}_H\big(\mathrm{Res}_H^G(V), W\big)$. Pour f dans l'espace de départ, soit $\Phi(f)$ l'application $V \to W$, $v \mapsto f(v)(e)$. Montrer que Φ est bien définie et linéaire.*
2. *On veut définir $\Psi : \mathrm{Hom}_H\big(\mathrm{Res}_H^G(V), W\big) \to \mathrm{Hom}_G\big(V, \mathrm{Ind}_H^G(W)\big)$. Pour r dans l'espace de départ, soit $\Psi(r)$ l'application qui envoie v de V sur l'élément $\Psi(r)(v) : G \to W$, $g \mapsto r(g \cdot v)$ de l'induit. Montrer que Ψ est bien définie et linéaire.*
3. *Montrer que Φ et Ψ sont deux applications réciproques l'une de l'autre.*

4. En déduire que l'on a :

$$\langle \chi_V, \chi_{\mathrm{Ind}_H^G(W)} \rangle_G = \langle \chi_{\mathrm{Res}_H^G(V)}, \chi_W \rangle_H .$$

Supposer d'abord que W et V sont irréductibles. Conclure dans le cas général par un argument de linéarité.

La loi de réciprocité de Frobenius *dit donc que si W et V sont irréductibles, alors V apparaît dans la décomposition de $\mathrm{Ind}_H^G(W)$ avec la même multiplicité que W dans la décomposition de $\mathrm{Res}_H^G(V)$.*

C.9. Exercice. *On exploite la réciprocité de Frobenius dans différents exemples où nous disposons de tables de caractères (exercice C.8).*

1. *On suppose ici que $H = \mathfrak{S}_2$ et $G = \mathfrak{S}_3$; on fixe une injection de H dans G. On notera 1_2 (resp. ε_2) la représentation triviale (resp. la signature) de H. On notera 1_3 (resp. χ_3, ε_3) la représentation triviale (resp. standard, signature) de G.*
   (a) *Montrer que* $\mathrm{Res}_H^G(1_3) = 1_2$, $\mathrm{Res}_H^G(\chi_3) = 1_2 + \varepsilon_2$, $\mathrm{Res}_H^G(\varepsilon_3) = \varepsilon_2$. Le caractère de $\mathrm{Res}_H^G(V)$, V irréductible se voit directement dans la table des caractères de G. Il faut avant tout connaître les décompositions $C_g \cap H$ des classes de conjugaison de G, intersectées avec H, en réunion de classes de conjugaison de H. Une fois connu le caractère (pour le groupe H), la décomposition en H-caractères irréductibles se fait directement grâce au corollaire X-B.9.
   (b) *En déduire que l'on a :* $\mathrm{Ind}_H^G(1_2) = 1_3 \oplus \chi_3$, $\mathrm{Ind}_H^G(\varepsilon_2) = \varepsilon_3 \oplus \chi_3$. On applique la réciprocité de Frobenius.
2. *On applique ici les mêmes méthodes. On suppose que $H = \mathfrak{S}_3$ et $G = \mathfrak{S}_4$; on fixe une injection de H dans G. On reprend la table des caractères du §6.2 en renommant les caractères de G : 1_4 (triviale), χ_4 (standard), ϕ_4 (appelée ϕ dans la table), χ_4^* (duale de la standard), ε_4 (signature).*
   (a) *Montrer les relations :*

$$\mathrm{Res}_H^G(1_4) = 1_3, \quad \mathrm{Res}_H^G(\chi_4) = 1_3 \oplus \chi_3, \quad \mathrm{Res}_H^G(\phi_4) = \chi_3,$$
$$\mathrm{Res}_H^G(\chi_4^*) = \varepsilon_3 \oplus \chi_3, \quad \mathrm{Res}_H^G(\varepsilon_4) = \varepsilon_3.$$

   (b) *En déduire les suivantes :*

$$\mathrm{Ind}_H^G(1_3) = 1_4 \oplus \chi_4, \quad \mathrm{Ind}_H^G(\chi_3) = \chi_4 \oplus \phi_4 \oplus \chi_4^*, \quad \mathrm{Ind}_H^G(\varepsilon_3) = \varepsilon_4 \oplus \chi_4^*.$$

C.10. Exercice (Réciprocité de Frobenius et action de G sur G/H)

Soit G un groupe fini et soit $H \subset G$ un sous-groupe. La réciprocité de Frobenius permet de décomposer la représentation $\mathbb{C}G/H$ de permutation pour l'action par multiplication à gauche de G sur G/H.

1. *Montrer, par l'exercice C.5, que la G-représentation $\mathbb{C}G/H$ est la représentation induite de la représentation triviale de H.*
2. *En déduire que la multiplicité de la G-représentation irréductible ρ dans $\mathbb{C}G/H$ est égale à la dimension du sous-espace des H-invariants dans la restriction $\rho|_H$, c'est-à-dire $\langle 1, \rho|_H\rangle_H$.*
3. *Retrouver, par exemple, le terme $2\theta_6$ dans la dernière question de l'exercice C.14.*

C.11. Exercice. *Retrouver les résultats de l'exercice X-F.49 en remarquant que la $\mathfrak{S}_4$-représentation V en question est l'induite de la représentation triviale du stabilisateur $\mathbb{Z}/4\mathbb{Z}$ d'une face du cube.*

Cf. l'exercice C.6 ou, mieux, l'exercice C.8 sur la réciprocité de Frobenius.

C.12. Exercice (Induction de sous-groupes d'indice 2)

On veut calculer l'induit de représentations irréductibles dans le cadre des sous-groupes d'indice 2. On supposera donc que H est un sous-groupe d'indice 2 du groupe fini G.

1. *Vérifier que l'on dispose d'une représentation non triviale ε de degré 1 par $G \to G/H \simeq \{\pm 1\}$. Pour toute représentation irréductible ρ, on a donc une représentation, également irréductible, $\varepsilon \otimes \rho$.*
2. *Montrer que $\chi_{\varepsilon\otimes\rho}(g) = \chi_\rho(g)$ si $g \in H$ et $\chi_{\varepsilon\otimes\rho}(g) = -\chi_\rho(g)$ si $g \notin H$. En développant et en éliminant les termes qui s'annulent, en déduire :*

$$|G|\langle\chi_\rho, \chi_\rho\rangle_G + |G|\langle\chi_\rho, \chi_{\varepsilon\otimes\rho}\rangle_G = 2|H|\langle\chi_{\rho|_H}, \chi_{\rho|_H}\rangle_H,$$

   où l'on note $\rho|_H$ la restriction de ρ à H.
3. *Montrer que l'on a deux possibilités :*
   (a) *soit $\rho \simeq \varepsilon \otimes \rho$; dans ce cas, $\langle\chi_{\rho|_H}, \chi_{\rho|_H}\rangle = 2$ et $\rho|_H$ se scinde en deux représentations irréductibles distinctes ;*
   (b) *soit $\rho \not\simeq \varepsilon \otimes \rho$; dans ce cas, $\langle\chi_{\rho|_H}, \chi_{\rho|_H}\rangle = 1$ et $\rho|_H$ reste irréductible.*
4. *On choisit un représentant s de $G\backslash H$ modulo H, et pour toute représentation irréductible π de H, on pose $\pi^s(g) = \pi(sgs^{-1})$. Déduire de la formule ($\heartsuit$) de l'exercice C.6 que de deux choses l'une :*
   (a) *soit $\pi \simeq \pi^s$, et dans ce cas $\mathrm{Ind}_H^G \pi$ se scinde en deux représentations irréductibles de G ;*
   (b) *soit $\pi \not\simeq \pi^s$, et dans ce cas $\mathrm{Ind}_H^G \pi$ est irréductible.*

5. *Observer ces résultats pour le groupe cyclique dans le groupe diédral, puis pour les couples suivants :* $\mathfrak{A}_3 \subset \mathfrak{S}_3$, $\mathfrak{A}_4 \subset \mathfrak{S}_4$, $\mathfrak{A}_5 \subset \mathfrak{S}_5$.

Signalons au passage que le *critère de Mackey* est une généralisation pour tout sous-groupe H de ce résultat.

C.13. Exercice (Représentations du groupe diédral D_n)

On rappelle que le groupe diédral D_n *est engendré par les générateurs* r *et* s*, soumis aux relations* $r^n = s^2 = (sr)^2 = e$.

1. *Montrer que les classes de conjugaison de* D_n *sont de la forme*

$$\{e\},\ \{r^k, r^{-k}\}\ \left(1 \leqslant k \leqslant \frac{n-1}{2}\right) \text{ et } \{s\}, \quad \text{pour } n \text{ impair,}$$

et

$$\{e\},\ \{r^k, r^{-k}\}\ \left(1 \leqslant k \leqslant \frac{n-2}{2}\right),\ \{r^{\frac{n}{2}}\},\ \{s\} \text{ et } \{rs\}, \quad \text{pour } n \text{ pair.}$$

2. *Montrer en utilisant la présentation fournie ci-dessus du groupe diédral qu'il possède deux, resp. quatre, représentations de degré* 1 *pour* n *impair, resp. pair.*

3. *En induisant à partir des représentations irréductibles du groupe cyclique d'ordre* n*, trouver la table de caractères de* D_n. On notera les deux sommes de carrés suivantes. Pour n impair : $2n = 2\times 1^2 + \frac{n-1}{2}\times 2^2$. Pour n pair : $2n = 4\times 1^2 + (\frac{n}{2}-1)\times 2^2$.

C.14. Exercice (Table des caractères de $\mathrm{GL}_3(\mathbb{F}_2)$)

Soit $G = \mathrm{GL}_3(\mathbb{F}_2) = \mathrm{PGL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. *On veut montrer que la table des caractères de* G *est :*

nom classe	1	2	3	4	7_1	7_2
cardinal classe	1	21	56	42	24	24
1	1	1	1	1	1	1
ϕ_3	3	-1	0	1	α	$\bar{\alpha}$
ϕ_3^*	3	-1	0	1	$\bar{\alpha}$	α
θ_6	6	2	0	0	-1	-1
ξ_7	7	-1	1	-1	0	0
η_8	8	0	-1	0	1	1

où $\alpha = (-1 + i\sqrt{7})/2$.

Pour rappel : l'étude des classes de conjugaison de G *est résumée dans le tableau page 266. On a aussi vu dans l'exercice I-C.21 que* G *possède un sous-groupe* H *d'ordre* 21 *isomorphe au produit semi-direct* $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$.

1. *Montrer, à l'aide de la proposition X-B.15, que l'action de* $\mathrm{PGL}_3(\mathbb{F}_2)$ *sur les sept droites de* $\mathbb{P}^2(\mathbb{F}_2)$ *fournit une représentation irréductible dont le caractère est* θ_6.

   On pensera à se servir des réalisations matricielles du tableau page 266 pour calculer les nombres d'invariants.

2. *Montrer de même que l'action de* $\mathrm{PSL}_2(\mathbb{F}_7)$ *sur les huit droites de* $\mathbb{P}^1(\mathbb{F}_7)$ *fournit une représentation irréductible dont le caractère est* ξ_7.

   On pensera à se servir des réalisations matricielles du tableau page 280 pour calculer les nombres d'invariants.

3. *Construction du caractère de degré* 8.

   (a) *Montrer que dans* H, *il y a six éléments d'ordre* 7 *et quatorze éléments d'ordre* 3.

   Comme $\mathbb{Z}/7\mathbb{Z}$ est distingué dans H, c'est le seul 7-Sylow.

   (b) *Soit* g *d'ordre* 3 *dans* H *et* C_g *sa classe de conjugaison dans* G. *Montrer que* $|C_g \cap H| = 14$, *puis que* $C_g \cap H$ *se décompose en deux classes de conjugaison sous* H.

   Pour la dernière question, remarquer que le groupe $\mathbb{Z}/7\mathbb{Z}$ agit non trivialement sur un élément d'ordre 3, car sinon, on aurait un produit direct.

   (c) *Soit* g *d'ordre* 7 *dans* H *et soit* C_g *sa classe de conjugaison dans* G. *Montrer que* g *et* g^{-1} *ne sont pas dans la même classe de conjugaison sous* G. *En déduire que* $|C_g \cap H| = 3$.

   Vu dans $\mathrm{GL}_3(\mathbb{F}_2)$, si le polynôme minimal de G est $X^3 + X + 1$, alors celui de g^{-1} est $X^3 + X^2 + 1$, et inversement : ils ne sont pas conjugués. En revanche, g^2 et g^4 sont conjugués à g par l'action d'un élément d'ordre 3 de H.

   (d) *Soit* $\bar{\eta}$ *la représentation de* H *donnée par* $\bar{\eta}(h) = \chi_j(\bar{h})$, *où* $\bar{h} \in \mathbb{Z}/3\mathbb{Z}$ *la classe de* h *modulo le 7-Sylow et soit* χ_j *le caractère de* $\mathbb{Z}/3\mathbb{Z}$ *donné par* $\chi_j(k) = j^k$ (j *est une racine cubique de* 1). *Montrer, en utilisant l'exercice C.6, que le caractère de l'induit de* $\bar{\eta}$ *de* H *à* G *est égal au caractère* η_8 *donné dans le tableau et qu'il est irréductible.*

4. *Construction des caractères de degré* 3.

   (a) *Montrer que les deux représentations restantes sont de degré* 3 *et sont données par les lignes* ϕ_3 *et* ϕ_3^* *du tableau.*

   Pour les degrés, on utilise la formule sur la somme des carrés. Pour les lignes, il manque pour toute colonne du tableau deux nombres a et b. L'orthogonalité des colonnes donne $3a + 3b$, donc $a + b$, et la norme des colonnes donne $a^2 + b^2$. Cela détermine a et b à permutation près.

(b) *Soit U un sous-groupe d'ordre 7 de G et soit $\varphi : U \to \mathbb{C}^*$ un caractère non trivial de degré 1. À l'aide de la réciprocité de Frobenius (exercice C.8), montrer que l'induit de φ de U à G est la somme de θ_6, ξ_7 et η_8 et d'un caractère irréductible de degré 3. Calculer ce caractère et terminer la table indépendamment de (a).*

Justifier par exemple :

$$\langle \theta_6, \mathrm{Ind}_U^G \varphi \rangle = \frac{1}{7}\Big(6\times 1 + \sum_{k=1}^{6}(-1)\times\zeta^k\Big) = 1, \text{ avec } \zeta^7 = 1 \text{ et } \zeta \neq 1.$$

5. *On fait agir $G = \mathrm{GL}_3(\mathbb{F}_2)$ sur la variété des drapeaux G/B de $\mathbb{F}_2^3$, ce qui fournit une représentation par permutation de degré 21, par [H2G2, proposition VIII-1.1]. Montrer que l'on retrouve la représentation η_8 comme facteur direct de cette représentation. Retrouver le résultat à l'aide de C.5 et de la réciprocité de Frobenius C.8.*

   Compter drapeaux stables pour chaque matrice du tableau page 266. Cela donne le caractère $[8,5,0,1,0,0]$, qui se décompose en $1+2\theta_6+\eta_8$.

6. *Les représentations irréductibles de degrés 1, 6 et 7 sont réelles (pourquoi ?). Vérifier de deux façons différentes que celle de degré 8 l'est aussi.*

   Utiliser l'indicateur de Frobenius-Schur de X-E.9 ou la question précédente.

Des représentations de $\mathbf{GL_2(\mathbb{F}_q)}$

C.15. Exercice (Caractères linéaires de $\mathbf{GL_2(\mathbb{F}_q)}$)

Soit $\mathbb{F}_q$ un corps de caractéristique distincte de 2. En utilisant le fait que le groupe dérivé de $\mathrm{GL}_2(\mathbb{F}_q)$ est $\mathrm{SL}_2(\mathbb{F}_q)$, montrer que $\mathrm{GL}_2(\mathbb{F}_q)$ possède exactement $q-1$ caractères de degré 1, et que ceux-ci sont donnés par les puissances du déterminant.

Les caractères de degré 1, appelés *caractères linéaires*, d'un groupe G sont ceux qui se factorisent par la projection $G \to G/[G,G]$, ils se déduisent des caractères du groupe abélien $G/[G,G]$; il y en a donc $|G/[G,G]|$. Les morphismes $g \mapsto \det^k(g)$ passent au quotient de $\mathrm{SL}_2(\mathbb{F}_q)$.

C.16. Exercice (Vers la série principale de représentations de $\mathbf{GL_2(\mathbb{F}_q)}$).

On note G le groupe $\mathrm{GL}_2(\mathbb{F}_q)$ et B le sous-groupe de G constitué des matrices triangulaires supérieures.

1. *Montrer que le groupe dérivé $[B,B]$ est le groupe de matrices unipotentes triangulaires supérieures et que $B/[B,B] \simeq (\mathbb{F}_q^*)^2$. On note dans la suite C_q le groupe des caractères du groupe abélien $(\mathbb{F}_q^*)^2$; on sait*

que C_q est (non canoniquement) isomorphe à $(\mathbb{F}_q^*)^2$. On identifiera donc C_q au groupe des caractères de degré 1 de B.

2. *Pour tout $\lambda \in C_q$, on note $V_\lambda = \mathrm{Ind}_B^G(\mathbb{C}_\lambda)$ et χ_λ son caractère, donné par la formule (♡) de l'exercice C.6. On veut calculer, pour tout g de G,*

$$\chi_\lambda(g) = \frac{1}{|B|} \sum_{\substack{p \in G \\ pgp^{-1} \in B}} \bar{\chi}_\lambda(pgp^{-1}) .$$

(a) Pour $g = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, montrer que

$$\chi_\lambda(g) = \frac{|G|}{|B|} \lambda(a,a) = (q+1)\lambda(a,a) .$$

(b) Pour $g = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, montrer que

$$\chi_\lambda(g) = \lambda(a,a) .$$

En considérant une matrice inversible p comme une matrice de passage, on voit que p envoie un sous-espace propre de g en un sous-espace propre de pgp^{-1}. Ainsi, dire que $pgp^{-1} \in B$ implique que p fixe la seule droite propre de g et donc que $p \in B$.

(c) Pour $g = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, avec $a \neq b$, montrer que

$$\chi_\lambda(g) = \lambda(a,b) + \lambda(b,a) .$$

Comme pour la question précédente, p envoie un sous-espace propre de g sur un sous-espace propre de pgp^{-1}. Si l'on note (e_1, e_2) la base canonique et D_i la droite engendrée par e_i, la condition $pgp^{-1} \in B$ donne deux possibilités : soit $p^{-1}(D_1) = D_1$, soit $p^{-1}(D_1) = D_2$, c'est-à-dire $p \in B$ ou $p \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in B$.

(d) Pour g non trigonalisable, montrer que $\chi_\lambda(g) = 0$.

Dans ce cas, g ne possède pas de droite propre, et il n'existe donc pas de p tel que $pgp^{-1} \in B$.

3. *On note D_q la diagonale $\{(\lambda_1, \lambda_1),\ \lambda_1 \in \mathbb{F}_q^*\}$ de C_q, identifié à $(\mathbb{F}_q^*)^2$. Montrer que $\langle \chi_\lambda, \chi_\lambda \rangle_G$ vaut 1 si $\lambda \notin D_q$ et 2 si $\lambda \in D_q$.*

C'est un calcul direct, qui utilise le tableau des classes de conjugaison de $\mathrm{GL}_2(\mathbb{F}_q)$, voir la proposition V-B.1, et les résultats précédents. On utilise le développement $|u+v|^2 = |u|^2 + |v|^2 + \bar{u}v + u\bar{v}$ ainsi que la formule de la série géométrique. À éviter après 23 h.

4. *Soit $\lambda = (\lambda_1, \lambda_1) \in D_q \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. Montrer que $V_\lambda = \mathbb{C}_{\lambda_1} \oplus W_\lambda$, où $\mathbb{C}_{\lambda_1}$ est le caractère linéaire $\det^{\lambda_1}$ et W_λ est une représentation irréductible de degré q.*

La représentation V_λ est de degré $[G : H] = q + 1$ et se décompose en deux composantes irréductibles. Il suffit donc de voir que $\mathbb{C}_{\lambda_1}$ en est une. On veut donc montrer que $\dim \mathrm{Hom}_G\big(\mathbb{C}_{\lambda_1}, \mathrm{Ind}_B^G(C_\lambda)\big) = 1$. Par le théorème de réciprocité de Frobenius (exercice C.8), il suffit de voir que la restriction de la représentation $\mathbb{C}_{\lambda_1}$ à B est $\mathbb{C}_\lambda$, ce qui est clair.

5. *Montrer que l'on a obtenu $(q-1)(q-2)/2$ représentations irréductibles distinctes de degré $q+1$ et $q-1$ représentations irréductibles distinctes de degré q.*

   L'irréductibilité ne fait pas de doute. On peut calculer les caractères grâce à ce qui précède et montrer qu'ils sont bien tous distincts.

Si l'on résume, le déterminant fournit $q-1$ caractères linéaires pour $\mathrm{GL}_2(\mathbb{F}_q)$ et l'induction fournit $q(q-1)/2$ caractères irréductibles non linéaires. D'après la proposition V-B.1, le groupe $\mathrm{GL}_2(\mathbb{F}_q)$ possède $q^2 - 1$ classes de conjugaison : il reste $q(q-1)/2$ caractères à dénicher. Cela se fait un peu plus péniblement en induisant les caractères linéaires du tore non déployé. Le lecteur assoiffé pourra se référer à [26, §5.25.4].

C.17. Exercice (Représentation de Steinberg)

On interprète de façon géométrique les $q-1$ représentations irréductibles W_λ de $\mathrm{GL}_2(\mathbb{F}_q)$ définies dans l'exercice C.16.

1. *Rappeler pourquoi l'action naturelle de $\mathrm{GL}_2(\mathbb{F}_q)$ sur la droite projective $X = \mathbb{P}^1(\mathbb{F}_q)$ est doublement transitive (et même triplement !) et en déduire que la représentation par permutation $\mathbb{C}X$ se décompose en $\mathbb{C}_{\mathrm{triv}} \oplus W$ avec W irréductible, appelée* représentation de Steinberg.

   L'action simplement transitive sur les repères projectifs ([H2G2, proposition XI-2.3.5]) permet de répondre à la question. La dernière assertion provient de la proposition X-B.15.

2. *En utilisant l'exercice C.5, montrer que W est isomorphe à la représentation $W_{(0,0)}$ de l'exercice C.16.*

   Le groupe G agit transitivement sur $\mathbb{P}^1(\mathbb{F}_q)$ et il existe une droite dont le stabilisateur est le sous-groupe B.

3. *En faisant agir le groupe des caractères linéaires sur W comme dans l'exercice X-F.22, montrer que l'on obtient toutes les autres représentations W_λ de l'exercice C.16.*

« As-tu la foi maintenant ?
— Non, mais je commence à cerner le problème ».
Kevin Smith, *Dogma*, 1999.

Chapitre XII

Épilogue : réalisation projective de $\mathfrak{A}_6$ et autres isomorphismes exceptionnels

Voici quelques derniers isomorphismes exceptionnels pour la route. Certains ont déjà été rencontrés, d'autres sont nouveaux. Nous allons construire, par des méthodes uniformes, les isomorphismes $\mathfrak{A}_6 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$, $\mathfrak{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$, $\mathfrak{A}_8 \simeq \mathrm{PSL}_4(\mathbb{F}_2)$. Tous ces isomorphismes passent par la « correspondance de Klein », c'est-à-dire, en passant par des groupes orthogonaux, (bien que l'on puisse aussi préférer le faire géométriquement, via des quadriques).

Il s'agit là d'un chapitre de synthèse avec au menu : la correspondance de Klein, les solides platoniciens, l'ordre des groupes orthogonaux sur un corps fini, l'utilisation des groupes simples, avec McKay en toile de fond et Galois en figure de proue.

En effet, les isomorphismes exceptionnels de groupes finis peuvent être vus comme des actions assez générales, donnant lieu à des injections d'un groupe projectif simple dans le groupe symétrique $\mathfrak{S}_n$, pour un n donné « assez petit ». Ces injections se trouvent, pour des raisons de petits cardinaux, être des isomorphismes sur le groupe $\mathfrak{A}_n$, ce qui permet de construire ces « exceptions ». Mais, dans une situation générale, ces injections s'envoient sur des sous-groupes de $\mathfrak{S}_n$ qui n'offrent aucune particularité. En revanche, on peut s'intéresser au nombre minimal n étiquetant le groupe $\mathfrak{S}_n$

dans lequel un groupe projectif simple, en particulier $\mathrm{PSL}_2(\mathbb{F}_p)$, peut s'injecter. Sachant que, pour des raisons évidentes de divisibilité, $\mathrm{PSL}_2(\mathbb{F}_p)$ ne peut s'injecter dans $\mathfrak{S}_n$ si $n < p$, et que, puisque $\mathrm{PSL}_2(\mathbb{F}_p)$ agit sur les $p+1$ droites de $\mathbb{F}_p^2$, il reste à comprendre les injections possibles de $\mathrm{PSL}_2(\mathbb{F}_p)$ dans $\mathfrak{S}_p$. On débouche alors sur une problématique qui rejoint la lettre de Galois. Ce sera notre dernière séquence émotion.

Commençons tout de suite par un petit mémento préliminaire. Pour rappel, voir le théorème IV-2.1. L'ordre $\mathfrak{o}_n^\zeta$ du groupe orthogonal $\mathrm{O}^\zeta(n,\mathbb{F}_q)$ de la forme quadratique de discriminant ζ sur $\mathbb{F}_q$ est donné par

$$\mathfrak{o}_{2n+1}^\zeta = 2q^n \prod_{k=0}^{n-1}(q^{2n}-q^{2k}), \quad \mathfrak{o}_{2n}^\zeta = 2(q^n - \varepsilon\alpha^n)\prod_{k=1}^{n-1}(q^{2n}-q^{2k}),$$

où $\varepsilon = \zeta^{(q-1)/2} \in \{1,-1\}$ et $\alpha = (-1)^{(q-1)/2} \in \{1,-1\}$.

On va construire par deux méthodes un isomorphisme exceptionnel entre $\mathfrak{A}_6$ et $\mathrm{PSL}_2(\mathbb{F}_9)$, ce qui permet entre autres d'expliquer l'automorphisme extérieur « exotique » de $\mathfrak{A}_6$ (qui provient alors tout simplement de l'action de $\mathrm{PGL}_2(\mathbb{F}_9)$ sur $\mathrm{PSL}_2(\mathbb{F}_9)$). On discutera ensuite de la généralisation des méthodes proposées à d'autres isomorphismes exceptionnels liés à la géométrie projective sur des corps finis.

Les méthodes proposées dans cette partie dévoilent un lien instructif entre la géométrie et la simplicité des groupes.

Nous aurons toutefois besoin d'admettre, voire de rappeler, quelques résultats de simplicité.

Proposition

(i) *Le groupe $\mathfrak{A}_n$ est simple pour $n \geqslant 5$;*

(ii) *le groupe $\mathrm{PSL}_2(\mathbb{F}_q)$ est simple pour $q \geqslant 4$;*

(iii) *le groupe dérivé $\Omega_3(q) = \mathrm{D}\,\mathrm{SO}_3(\mathbb{F}_q)$ est simple pour $q \geqslant 4$.*

Démonstration. Voir [65, chapitres I et IV] et, pour la dernière propriété, [73, §XXI 4.2.10]. □

1. Méthode naturelle

1.1. Théorème. *Les groupes finis simples suivants sont isomorphes :*

$$\mathfrak{A}_6 \simeq \mathrm{PSL}_2(\mathbb{F}_9).$$

Démonstration. On va donner une construction naturelle, et dont le caractère canonique sera laissé à l'appréciation du lecteur[1], de l'isomorphisme

[1] Ayant un point de vue opposé sur le sujet, nous nous contenterons, au titre d'auteurs, de dire que l'isomorphisme obtenu est canonique, mais pas trop.

exceptionnel $\mathfrak{A}_6 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$. Pour cela notons que le groupe $\mathfrak{S}_6$ agit canoniquement sur k^6 par permutation des coordonnées pour tout corps k et ce, en préservant la forme quadratique canonique (non dégénérée) $q_c = \sum_{i=1}^6 x_i^2$. Soit D la droite canonique engendrée par $(1,\dots,1)$ et soit H son orthogonal pour q_c. On travaille maintenant sur $k = \mathbb{F}_3$ afin d'avoir $D \subset D^\perp = H$. Ainsi, le noyau de la forme $q_c|_H$ est D, et l'on récupère une forme quadratique non dégénérée q sur le quotient H/D de dimension 4 donnée par $q(h+D) = q(h)$, sachant qu'il s'agit comme il va de soi de vérifier au préalable qu'elle est bien définie. De plus, l'action de $\mathfrak{S}_6$ stabilise H et D, donc H/D, et finalement stabilise la forme q. On vient donc de définir, via cette action, un morphisme ϕ de $\mathfrak{S}_6$ vers $\mathrm{O}(q)$.

Étudions maintenant la forme quadratique q. On sait que q est non dégénérée sur un espace de dimension 4 et que $\mathfrak{A}_6$ s'envoie (non trivialement, bien sûr) sur $\mathrm{O}(q)$. Comme $\mathfrak{A}_6$ est simple, il s'injecte dans $\mathrm{O}(q)$. Or, par les formules rappelées plus haut, les ordres des groupes orthogonaux des deux formes quadratiques non dégénérées en dimension 4 sur $\mathbb{F}_3$ sont 16×72, pour la forme de discriminant 1, et 20×72, pour celle de discriminant -1. Le groupe $\mathfrak{A}_6$ ne peut s'injecter (par Lagrange) que dans le groupe $\mathrm{O}_4^-(\mathbb{F}_3)$, si bien que le discriminant de q est de signature -1.

Maintenant, comme $\mathfrak{A}_6$ est simple non abélien, le groupe dérivé $\mathrm{D}(\mathfrak{A}_6)$ est égal à $\mathfrak{A}_6$, et l'injection de $\mathfrak{A}_6$ dans O_4^- fournit donc un morphisme injectif de $D(\mathfrak{A}_6) = \mathfrak{A}_6$ dans $D\big(\mathrm{O}_4^-(\mathbb{F}_3)\big) \subset \mathrm{SO}_4^-(\mathbb{F}_3)$, de sorte que $\mathfrak{A}_6$ s'envoie injectivement dans $\mathrm{SO}_4^-(\mathbb{F}_3) = \mathrm{SO}_4^{-1}(\mathbb{F}_3)$. En composant le morphisme obtenu par la projection canonique sur $\mathrm{PSO}_4^-(\mathbb{F}_3) = \mathrm{SO}_4^-(\mathbb{F}_3)/\{\pm 1\}$, on obtient un morphisme injectif, car $\mathfrak{A}_6$ est simple, et, par cardinalité, ce morphisme est surjectif vu que $20 \times 72/4 = 6!/2$. On a montré l'isomorphisme canonique entre $\mathfrak{A}_6$ et $\mathrm{PSO}_4^-(\mathbb{F}_3)$. L'isomorphisme $\mathrm{PSO}_4^-(\mathbb{F}_3) \simeq \mathrm{PSL}_2(\mathbb{F}_9)$ est standard, voir le lemme qui suit. □

1.2. Lemme. *Si q est congru à 3 modulo 4, on a un isomorphisme*

$$\mathrm{PSL}_2(\mathbb{F}_{q^2}) \simeq \mathrm{PSO}_4^-(\mathbb{F}_q),$$

provenant de l'action de $\mathrm{SL}_2(\mathbb{F}_{q^2})$ par congruence hermitienne sur le $\mathbb{F}_q$-espace $\mathscr{H}_2(\mathbb{F}_{q^2}) = \{H \in \mathscr{M}_2(\mathbb{F}_{q^2}),\ {}^tH^q = H\}$ des matrices hermitiennes.

Démonstration. On rappelle que l'automorphisme de Frobenius $F : x \mapsto x^q$ est un isomorphisme involutif de $\mathbb{F}_{q^2}$. On peut donc définir sur l'espace des matrices un anti-automorphisme d'algèbres d'adjonction $?^* : M \mapsto M^* = {}^tM^q$ (cela revient à transposer M et à appliquer le Frobenius F composante par composante). On considère l'action, dite de congruence hermitienne, de $\mathrm{SL}_2(\mathbb{F}_{q^2})$ sur $\mathscr{H}_2(\mathbb{F}_{q^2})$ donnée par $P \cdot H = PHP^*$. On vérifie que l'action est bien définie, que cette action stabilise le déterminant, qui

est une forme quadratique sur le $\mathbb{F}_q$-espace $\mathscr{H}_2(\mathbb{F}_{q^2})$ de dimension 4. Pour calculer cette forme quadratique on remarque d'abord que, comme q est congru à 3 modulo 4, on a $(-1)^{(q-1)/2} = -1$, et donc -1 n'est pas un carré de $\mathbb{F}_q$. Ainsi, $\mathbb{F}_{q^2} = \mathbb{F}_q[i]$, où i est une racine de -1 (l'autre racine étant $-i = i^q$). Une matrice hermitienne et son déterminant sont donnés par

$$H = \begin{pmatrix} a & c-id \\ c+id & b \end{pmatrix}, \quad a,b,c,d \in \mathbb{F}_q, \ \det H = ab - c^2 - d^2.$$

L'expression de la forme det montre qu'il s'agit d'une forme quadratique de discriminant -1. Et, comme le noyau de l'action est donné par les homothéties, voir [H2G2, proposition V-B.2.2] dans le cas symétrique, très analogue, on a le morphisme injectif $\mathrm{PSL}_2(\mathbb{F}_{q^2}) \hookrightarrow \mathrm{O}_4^-(\mathbb{F}_q)$. Le groupe $\mathrm{PSL}_2(\mathbb{F}_{q^2})$ étant simple non abélien, ce morphisme fournit un morphisme de $D\big(\mathrm{PSL}_2(\mathbb{F}_{q^2})\big) = \mathrm{PSL}_2(\mathbb{F}_{q^2})$ dans $D\big(\mathrm{O}_4^-(\mathbb{F}_q)\big) \subset \mathrm{SO}_4^-(\mathbb{F}_q)$. On compose par la surjection canonique pour obtenir un morphisme (non trivial, donc injectif) de $\mathrm{PSL}_2(\mathbb{F}_{q^2})$ dans $\mathrm{PSO}_4^-(\mathbb{F}_q)$. Par égalité des cardinaux, on obtient un isomorphisme. □

1.3. Remarque. Pour une généralisation à l'aide d'une méthode élégante qui utilise les algèbres de Clifford, voir [73, proposition XXVII-4.2.4].

1.4. Remarque. Avant d'oublier. Grâce au corollaire IV-2.6, on voit que la quadrique $q(x) = 0$ a pour cardinal 21 (une quadrique associée à q de discriminant 1 aurait pour cardinal 33) et donc la quadrique projective $Q \subset \mathbb{P}^3(\mathbb{F}_3)$ est de cardinal 10. Dans Q, identifié à $\mathbb{P}(H/D)$, la classe du point $(1,1,1,0,0,0)$ est égale à celle du point $(0,0,0,1,1,1)$. On voit alors que Q est en bijection naturelle avec l'ensemble $\mathscr{P}_{3,3}$ des partitions de $\{1,\dots,6\}$ en deux parties à trois éléments.

Une autre façon de voir consiste à remarquer que l'ensemble des 3-Sylow de $\mathfrak{A}_6$ est en bijection naturelle avec $\mathscr{P}_{3,3}$ et ainsi, on réalise l'action de $\mathfrak{A}_6$ sur $\mathscr{P}_{3,3}$ par l'action par conjugaison de $\mathfrak{A}_6$ sur l'ensemble de ses 3-Sylow.

On voit ainsi que l'isomorphisme exceptionnel $\mathfrak{A}_6 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$ que nous venons de montrer provient d'une structure (ingénieuse) de $\mathbb{F}_9$-espace projectif sur $\mathscr{P}_{3,3}$.

2. Méthode géométrique

On se propose à nouveau de montrer l'isomorphisme $\mathfrak{A}_6 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$, mais cette fois-ci à l'aide des solides platoniciens, ou plutôt, d'une version de ces solides adaptée aux corps finis. Voici donc une méthode qui ne manque pas de charme bien qu'elle manque cruellement de canonicité. On en présente un aperçu dans une version compacte maximale.

La preuve commence mystérieusement par la remarque que 5 possède deux racines carrées dans $\mathbb{F}_9$, que l'on note $\pm\alpha$, ce qui permet de construire le nombre d'or[2] $\phi = 2^{-1}(1+\alpha)$ dans $\mathbb{F}_9$ (cette remarque prononcée doctement avec l'index levé vous ouvrira la porte des sectes les plus ésotériques). (C'est même vrai pour p premier impair : toute classe d'entiers non nulle dans $\mathbb{F}_p$ possède deux racines carrées dans l'extension $\mathbb{F}_{p^2}$, par unicité de l'extension quadratique de $\mathbb{F}_p$.) On peut donc construire un « icosaèdre » dans $\mathbb{F}_9^3$ dont les douze sommets[3] sont $(\pm\phi, \pm 1, 0)$, $(0, \pm\phi, \pm 1)$, $(\pm 1, 0, \pm\phi)$. C'est un « polyèdre régulier » P pour la forme quadratique canonique $Q = \sum_{j=1}^{3} x_j^2$. Pour donner un sens à « régulier », on définit les arêtes et les faces de P comme des parties à deux ou trois éléments de P, comme dans $\mathbb{R}^3$, alors le groupe d'isométrie de P est inclus dans le groupe orthogonal de la forme quadratique et il agit de façon transitive sur les *drapeaux* formés d'un point appartenant à une arête incluse dans une face.

On trouve le théorème suivant dans [73, §XXI-4.2.9 et 4.2.10]. Pour le cas où $q = 3$, on pourra se référer à l'exercice 3.1.

2.1. Théorème. *Soit $q \neq 3$. Le groupe $\mathrm{SO}_3(\mathbb{F}_q)$ possède un unique sous-groupe simple $\Omega_3(\mathbb{F}_q)$ d'indice 2 ; c'est le sous-groupe dérivé de $\mathrm{SO}_3(\mathbb{F}_q)$.*

Nous allons en déduire un isomorphisme $\mathfrak{A}_6 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$. Considérons l'orbite $\Omega_3(\mathbb{F}_9)\cdot P$ constituée d'icosaèdres réguliers inscrits sur la nappe d'équation $Q(x)=\phi^2+1$. L'idée est, comme nous allons le démontrer, qu'il y a six icosaèdres dans cette orbite, ce qui donne un morphisme de $\Omega_3(\mathbb{F}_9)$ dans $\mathfrak{S}_6$.

Il faut maintenant passer au calcul du cardinal k de l'orbite de P, c'est-à-dire, déterminer le stabilisateur $\Omega_3(\mathbb{F}_9)_P$ de P. Rappelons que dans le cas réel, le stabilisateur $\mathrm{SO}_3(\mathbb{R})_P$ est $\mathfrak{A}_5$ (voir [H2G2, proposition XII-3.16] et se souvenir que l'icosaèdre est le dual du dodécaèdre). Montrons que c'est aussi le cas dans le groupe $\Omega_3(\mathbb{F}_9)$.

On se convainc d'abord que l'on peut retrouver le groupe $\mathfrak{A}_5$ dans $\mathrm{SO}_3(\mathbb{F}_9)_P$: les matrices des éléments de $\mathfrak{A}_5$ agissant sur $\mathbb{R}^3$ ont leurs coefficients dans l'anneau $R = \mathbb{Z}\big[1/2, \sqrt{5}\big]$, ce qui permet de les réduire via un (des deux) morphisme(s) $R \to \mathbb{F}_9$: voir l'exercice X-F.48. On réalise ainsi $\mathfrak{A}_5$ comme un sous-groupe de $\mathrm{SO}_3(\mathbb{F}_9)$ qui stabilise P.

Montrons à présent que $\mathfrak{A}_5 \subset \mathrm{SO}_3(\mathbb{F}_9)_P$ s'injecte, plus précisément, dans $\Omega_3(\mathbb{F}_9)$. Pour cela, on considère $\mathfrak{A}_5 \cap \Omega_3(\mathbb{F}_9)$: c'est soit $\mathfrak{A}_5$, soit un sous-groupe d'indice 2 dans $\mathfrak{A}_5$, mais ce dernier cas est impossible sinon $\mathfrak{A}_5$ posséderait un sous-groupe distingué. D'où l'inclusion $\mathfrak{A}_5 \subset \Omega_3(\mathbb{F}_9)$.

[2] On devrait dire « un » nombre d'or, car on ne peut pas distinguer les deux racines carrées de 5.

[3] Ces points de $\mathbb{F}_9^3$ sont bien distincts — pourquoi ?

Supposons maintenant que l'inclusion $\mathfrak{A}_5 \subset \Omega_3(\mathbb{F}_9)_P$ soit stricte. Alors, comme $|\Omega_3(\mathbb{F}_9)| = 9(9^2-1)/2 = 360$ d'après nos formules d'ordre, on aurait $k < 360/60 = 6$. Dans ce cas, on aurait un morphisme non trivial de $\Omega_3(\mathbb{F}_9)$ vers $\mathfrak{S}_k$, nécessairement injectif, car $\Omega_3(\mathbb{F}_9)$ est simple. Cela est impossible, car $360 > 5! = 120$. Ainsi, $k = 6$ et $\Omega_3(\mathbb{F}_9)$ s'envoie injectivement dans $\mathfrak{S}_6$. Comme son image est d'indice 2 dans $\mathfrak{S}_6$, le groupe $\Omega_3(\mathbb{F}_9)$ est isomorphe à $\mathfrak{A}_6$.

Nous venons donc de voir que $\mathfrak{A}_6$ est isomorphe à $\Omega_3(\mathbb{F}_9)$. Il reste à montrer que $\Omega_3(\mathbb{F}_9)$ est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_9)$. La correspondance de Klein, voir aussi [H2G2, proposition IX-2.1] pour le cas complexe, assure l'isomorphisme entre $\mathrm{PSL}_2(\mathbb{F}_9)$ et $\Omega_3(\mathbb{F}_9)$. Rappelons rapidement comment cela s'obtient : $\mathrm{SL}_2(\mathbb{F}_9)$ agit par conjugaison sur l'espace des matrices 2×2 de trace nulle sur $\mathbb{F}_9$, et l'action préserve le déterminant. Une telle matrice et son déterminant peuvent s'écrire

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \text{ (où } a, b, c, d \in \mathbb{F}_9\text{)}, \ \det A = -a^2 - bc.$$

L'action préserve donc une forme quadratique de discriminant 1 en dimension 3. Cela fournit un morphisme de $\mathrm{SL}_2(\mathbb{F}_9)$ vers $\mathrm{O}_3(\mathbb{F}_9)$ dont le noyau est le groupe des homothéties. La simplicité de $\mathrm{PSL}_2(\mathbb{F}_9)$ implique que son image est bien le sous-groupe $\Omega_3(\mathbb{F}_9)$ (en passant le morphisme obtenu aux sous-groupes dérivés), qui est d'indice 4 dans $\mathrm{O}_3(\mathbb{F}_9)$.

3. La lettre de Galois

> « Il est curieux de savoir si le degré peut s'abaisser. Et, d'abord, il ne peut s'abaisser plus bas que p, puisqu'une équation de degré moindre que p, ne peut avoir p pour facteur dans le nombre des permutations de son groupe. Voyons donc si l'équation de degré $p+1$ [...] peut s'abaisser au degré p. [...] Ainsi, pour le cas de $p = 5, 7, 11$, l'équation modulaire s'abaisse au degré p. En toute rigueur, cette réduction n'est pas possible dans les cas plus élevés. Ces deux méthodes sont suffisamment générales pour que l'on soit tenté de les appliquer à d'autres résultats analogues. En réalité, elles se généralisent toutes deux de façon élégante, mais dans deux directions différentes. [...] Tu prieras publiquement Jacobi ou Gauss de donner leur avis non sur la vérité, mais sur l'importance des théorèmes. Après cela il se trouvera, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis. »
>
> Évariste Galois, lettre à Auguste Chevalier, 29 Mai 1832.

La première méthode utilisée au §1 permet d'obtenir de manière analogue tous les isomorphismes exceptionnels entre les groupes alternés $\mathfrak{A}_n$ et les autres groupes finis simples de la classification. Donnons-en un aperçu pour les moins faciles.

L'isomorphisme $\mathfrak{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$ s'obtient en considérant l'action naturelle de $\mathfrak{A}_5$ sur $\mathbb{F}_5^5$ respectant la forme quadratique canonique $\sum_i x_i^2$ que l'on restreint et passe au quotient sur l'espace canonique H/D de dimension 3. On obtient alors un isomorphisme $\mathfrak{A}_5 \simeq \Omega_3(\mathbb{F}_5)$ puis, par la correspondance de Klein, $\mathfrak{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$ comme désiré.

L'isomorphisme $\mathfrak{A}_8 \simeq \mathrm{PSL}_4(\mathbb{F}_2)$ s'obtient en considérant l'action naturelle de $\mathfrak{A}_8$ sur $\mathbb{F}_2^8$ respectant la forme quadratique canonique $\sum_{i<j} x_i x_j$ que l'on restreint et passe au quotient sur l'espace canonique H/D de dimension 6. On obtient ainsi un isomorphisme $\mathfrak{A}_8 \simeq \Omega_6^+(\mathbb{F}_2)$ qui par le morphisme $\mathrm{PSL}_4 \simeq \mathrm{SO}_6$ donné par le pfaffien fournit $\mathfrak{A}_8 \simeq \mathrm{PSL}_4(\mathbb{F}_2)$ (voir le paragraphe VI-2, mais voir aussi [73, chapitre XXX] pour une généralisation à la caractéristique 2). On trouvera en 3.4 une preuve alternative élémentaire de ce résultat.

La seconde méthode donne une démarche générale pour construire toutes les actions exceptionnelles (non triviales) de $\mathrm{PSL}_2(\mathbb{F}_p)$ sur un ensemble à moins de $p+1$ éléments lorsque p est premier. On sait depuis la fameuse lettre testamentaire d'Évariste Galois (citée partiellement ci-dessus) que les exceptions se produisent uniquement pour $p \in \{2, 3, 5, 7, 11\}$ et dans ces cas $\mathrm{PSL}_2(\mathbb{F}_p)$ agit transitivement sur un ensemble à p éléments. Par ailleurs, comme le fait remarquer Galois dans sa lettre, un morphisme de $\mathrm{PSL}_2(\mathbb{F}_p)$ dans $\mathfrak{S}_k$, $k < p$ serait forcément trivial, par le théorème de Lagrange et par simplicité du groupe. Regardons comment les choses peuvent se montrer dans les cas $p = 11$, puis 7.

Si $p = 11$, le nombre d'or est encore un élément de $\mathbb{F}_{11}$ puisque le symbole de Legendre 5^5 vaut 1 modulo 11. On peut donc construire un icosaèdre dans $\mathbb{F}_{11}$ et montrer comme précédemment que son stabilisateur dans $\Omega_3(\mathbb{F}_{11}) \simeq \mathrm{PSL}_2(\mathbb{F}_{11})$ contient comme sous-groupe $\mathfrak{A}_5$. Or, $|\mathrm{PSL}_2(\mathbb{F}_{11})| = (11+1) \times 11 \times (11-1)/2 = 660$. Ainsi, $\mathrm{PSL}_2(\mathbb{F}_{11})$ agit transitivement sur le quotient $\mathrm{PSL}_2(\mathbb{F}_{11})/\mathfrak{A}_5$, de cardinal 11.

Il faut une légère variante pour le cas $p = 7$ puisque, cette fois-ci, 5 n'est pas un carré dans $\mathbb{F}_7$. En revanche, on peut toujours construire un cube dans $\mathbb{F}_7^3$ avec les sommets $(\pm 1, \pm 1, \pm 1)$. Le stabilisateur du cube dans $\mathrm{SO}_3(F_7)$ contient donc le groupe $\mathfrak{S}_4$ qui permute les quatre « grandes » diagonales du cube. Mais la méthode précédente utilisait le fait que $\mathfrak{A}_5$ est simple, alors que $\mathfrak{S}_4$ ne l'est pas. En revanche, la correspondance de Klein donne toujours l'isomorphisme entre groupes simples $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \Omega_3(F_7)$. Donc, si l'on peut montrer que $\mathfrak{S}_4$ est plus précisément un sous-groupe de $\Omega_3(F_7)$, alors on obtient un ensemble-quotient $\Omega_3(F_7)/\mathfrak{S}_4$ sur lequel $\mathrm{PSL}_2(\mathbb{F}_7)$ agit et de cardinal $(7+1) \times 7 \times (7-1)/(2 \times 24) = 7$, comme désiré.

Montrons donc cette assertion. Pour cela, il suffit de voir cette propriété pour les générateurs de $\mathfrak{S}_4$. Rappelons que les transpositions de $\mathfrak{S}_4$ sont

réalisées par les rotations (d'ordre 2 !) passant par les milieux d'arêtes opposées. Par symétrie, il suffit de la montrer pour une seule telle rotation. Choisissons donc le renversement par rapport à la droite engendrée par $(1,1,0)$, qui peut être vu comme composé des symétries par rapport aux plans $z=0$ et $x-y=0$. Les axes orthogonaux de ces plans sont donc respectivement $u=(0,0,1)$ et $v=(1,-1,0)$ et l'on a pour la forme quadratique canonique q que $q(u)=1$ et $q(v)=2$ sont des carrés de $\mathbb{F}_7$. Ainsi, la rotation est composée de symétries dont les axes sont engendrés par des vecteurs x tels que $q(x)$ est un carré non nul, et donc cette rotation est bien dans $\Omega_3(\mathbb{F}_7)$ (voir [73, théorème XXII-3.0.3]).

Pour le cas $p=5$, on réalise que cette construction via le cube ne marche pas, car 2 n'est plus un carré. En revanche, on peut construire un tétraèdre et obtenir $\mathfrak{A}_4$ d'indice 5 dans $\mathrm{PSL}_2(\mathbb{F}_5)$. On devine, à travers la présence de ces solides platoniciens, la correspondance McKay (voir les chapitres XI et XI-8) derrière ces cinq cas exceptionnels.

3.1. Exercice. *Par le théorème IV-2.1, on voit que l'ordre de* $\mathrm{SO}_3(\mathbb{F}_3)$ *est* 24.

1. *Montrer que ce groupe est isomorphe à* $\mathfrak{S}_4$ *en le faisant agir sur les quatre « grandes diagonales » du cube de* $\mathbb{F}_3^3$ *donné par les huit sommets* $(\pm1,\pm1,\pm1)$. *En déduire le sous-groupe dérivé de* $\mathrm{SO}_3(\mathbb{F}_3)$.
   Soit $q=x_1^2+x_2^2+x_3^2$ la forme quadratique canonique de $\mathbb{F}_3^3$. On pourra noter que pour un vecteur directeur x des axes de symétrie du cube, $q(x)$ vaut 0, -1 ou 1, si l'axe joint, respectivement, deux sommets opposés, deux milieux d'arêtes opposées, ou deux centre de faces opposées.
2. *Montrer que le sous-groupe* V *de* $\mathrm{SO}_3(\mathbb{F}_3)$, *engendré par les réflexions par rapport aux axes engendrés par des vecteurs de* (x_1,x_2,x_3) *de* $\mathbb{F}_3^3$ *tels que* $x_1^2+x_2^2+x_3^2=1$, *est isomorphe au groupe de Klein.*

3.2. Remarque. On sait, voir [H2G2, proposition XII-3.12], que le groupe des isométries du tétraèdre régulier est isomorphe à $\mathfrak{S}_4$. Dans cet isomorphisme, la signature d'une permutation de $\mathfrak{S}_4$ correspond au déterminant de l'isométrie. On sait également, [H2G2, proposition XII-3.12], que le groupe des isométries positives du cube est isomorphe à $\mathfrak{S}_4$. On peut alors se demander à quel invariant correspond la signature d'une permutation. Certainement pas au déterminant, puisque celui-ci vaut toujours 1 sur les isométries positives. L'exercice précédent donne une idée de la réponse : il s'agit de la *norme spinorielle*, voir [73, chapitre XXII].

3.3. Exercice (Une preuve express de l'isomorphisme $\mathrm{PSL}_2(\mathbb{F}_7)\simeq\mathrm{GL}_3(\mathbb{F}_2)$). *Voici probablement une des preuves élémentaires les plus rapides de l'existence de l'isomorphisme exceptionnel* $\mathrm{PSL}_2(\mathbb{F}_7)\simeq\mathrm{GL}_3(\mathbb{F}_2)$.

On rappelle que le groupe $\mathrm{PSL}_2(\mathbb{F}_7)$ *agit fidèlement par homographie sur les huit droites de* $\mathbb{P}^1(\mathbb{F}_7) = \{0, 1, \dots, 6, \infty\}$, *et qu'il est engendré par* $\sigma : z \mapsto z+1$, *d'ordre 7, et* $\tau : z \mapsto -1/z$, *d'ordre 2. Ainsi, on identifie* $\mathrm{PSL}_2(\mathbb{F}_7)$ *à un sous-groupe de* $\mathfrak{S}\big(\mathbb{P}^1(\mathbb{F}_7)\big)$, σ *à la permutation* (0123456) *et* τ *à* $(0\infty)(16)(23)(45)$. *On pose* $\alpha = (15)(23)(46)(0\infty)$.

1. *Montrer par le calcul que* $\beta = \sigma\alpha\sigma^{-1}$ *commute avec* α. *Montrer également que si l'on pose* $\gamma = \sigma\beta\sigma^{-1}$, *alors* $\sigma\gamma\sigma^{-1} = \alpha\gamma$.
2. *En déduire que l'orbite* $\mathscr{O}$ *du sous-groupe* $\langle\sigma\rangle$ *par conjugaison sur* α *constitue, avec l'identité, un sous-groupe* A *de* $\mathfrak{S}\big(\mathbb{P}^1(\mathbb{F}_7)\big)$ *isomorphe à* $\mathbb{F}_2^3$.

   Comme α et β commutent, tout élément κ de l'orbite de α commute avec $\sigma\alpha\sigma^{-1}$. Après simplification, on trouve successivement α, β, γ, $\alpha\gamma$, $\beta\alpha\gamma$, $\beta\alpha$, $\gamma\beta$. Ils sont bien sûr tous d'ordre 2, et l'on vérifie qu'ils commutent. Cela nous donne l'isomorphisme voulu.
3. *Montrer que la conjugaison par* τ *fixe* α *et* γ *et envoie* β *sur* $\alpha\beta\gamma$. *En déduire une représentation fidèle de* $\mathrm{PSL}_2(\mathbb{F}_7)$ *de degré 3 sur* $\mathbb{F}_2$, i.e. *un morphisme injectif de* $\mathrm{PSL}_2(\mathbb{F}_7)$ *dans* $\mathrm{GL}_3(\mathbb{F}_2)$.

   On voit par les calculs proposés que τ stabilise l'orbite $\mathscr{O}$. Donc, le groupe engendré par σ et τ, c'est-à-dire $\mathrm{PSL}_2(\mathbb{F}_7)$, stabilise $\mathscr{O}$ et donc le sous-groupe A. Comme l'action par conjugaison se fait par automorphismes, on en déduit que l'action de $\mathrm{PSL}_2(\mathbb{F}_7)$ est linéaire sur $\mathbb{F}_2^3$, d'où un morphisme $\mathrm{PSL}_2(\mathbb{F}_7) \to \mathrm{GL}_3(\mathbb{F}_2)$, forcément injectif par simplicité de $\mathrm{PSL}_2(\mathbb{F}_7)$.
4. *En déduire l'isomorphisme proposé.*

   Par cardinalité !

3.4. Exercice (Isomorphisme $\mathrm{GL}_4(\mathbb{F}_2) \simeq \mathfrak{A}_8$)

Voici une méthode convaincante (à défaut d'être éclairante) pour cet isomorphisme exceptionnel. On commence par une présentation du groupe alterné $\mathfrak{A}_{n+2}$ *pour* n *entier non nul quelconque.*

1. *Soient* i *et* j *des entiers distincts compris entre 3 et* $n+2$. *Dans le groupe alterné* $\mathfrak{A}_{n+2}$, *calculer le produit* $\alpha = (12i)(12j)$, *puis* $\alpha(12k)\alpha^{-1}$ *où* $k \notin \{1, 2, i, j\}$. *En déduire que les 3-cycles* $(12i)$ $(3 \leqslant i \leqslant n+2)$ *engendrent* $\mathfrak{A}_{n+2}$.

   On rappelle que les 3-cycles engendrent $\mathfrak{A}_{n+2}$.
2. *On note* G_n *le groupe présenté par générateurs* $x_1, \dots, x_n$ *et relations*

$$\forall i,\ x_i^3 = 1; \quad \forall i, j,\ i \neq j,\ (x_i x_j)^2 = 1.$$

   Montrer qu'il existe un morphisme surjectif $G_n \to \mathfrak{A}_{n+2}$.

   Utiliser la propriété universelle des groupes libres : il suffit de vérifier que les 3-cycles $(12i)$ satisfont aux mêmes relations que les x_i.

3. *Soit H le sous-groupe de G_n engendré par x_i $(1 \leqslant i \leqslant n-1)$. Montrer que l'ensemble $H \cup x_n H \cup x_n^2 H \cup x_1 x_n^2 H \cup \cdots \cup x_{n-1} x_n^2 H$ est stable par multiplication à gauche par les x_i, puis que cet ensemble est G_n tout entier.*

   La stabilité se fait en utilisant les relations de G_n. Pour finir, constater que le seul ensemble contenant le neutre et stable par multiplication à gauche par les générateurs est G_n.

4. *Montrer par récurrence, en majorant le cardinal de l'ensemble quotient G_n/H, que G_n est isomorphe à $\mathfrak{A}_{n+2}$.*

5. *Montrer que l'ordre de $\mathrm{GL}_4(\mathbb{F}_2)$ est égal à celui de $\mathfrak{A}_8$.*

6. *Montrer l'isomorphisme de groupes $\mathrm{GL}_4(\mathbb{F}_2) \simeq \mathfrak{A}_8$, en considérant les matrices suivantes de $\mathrm{GL}_4(\mathbb{F}_2)$:*

$$b_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad b_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \quad b_3 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

$$b_4 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad b_5 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad b_6 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

   Un calcul simple mais un peu fastidieux montre que les b_i satisfont aux relations — un logiciel de calcul formel comme Sage peut aider ; on peut même le programmer pour *trouver* des matrices comme les b_i.

— As Bertrand Russell once said,
"the only thing that will redeem mankind is cooperation".
I think we can all appreciate the relevance of that now.
— Was that on a beer mat?
— Yeah, it was Guinness Extra Cold.
Edgar Wright, *Shaun of the dead*, 2004.

Bibliographie

[H2G2] (*) Philippe CALDERO et Jérôme GERMONI : *Histoires hédonistes de groupes et de géométries – Tome premier.* Mathématiques en devenir. Calvage et Mounet, Paris, 2013.

[1] Roger C. ALPERIN : The modular tree of Pythagoras. *Amer. Math. Monthly*, 112(9):807–816, 2005. Disponible en ligne : `http://www.math.sjsu.edu/~alperin/pt.pdf`.

[2] Aurélien ALVAREZ, Étienne GHYS et Jos LEYS : *Dimensions. Une promenade mathématique*, 2008. Film d'animation et site disponibles en ligne : `http://dimensions-math.org/`.

[3] Emil ARTIN : *Algèbre géométrique.* Les Grands Classiques Gauthier-Villars. Éditions Jacques Gabay, Paris, 1996. Traduit de l'édition originale de 1957 par M. Lazard, édition et préface de G. Julia.

[4] Michèle AUDIN : *Géométrie.* EDP-Sciences, Grenoble, deuxième édition, 2006.

[5] Michèle AUDIN : *Analyse complexe*, 2011. Notes d'un cours donné à l'Université de Strasbourg, disponible en ligne : `http://www-irma.u-strasbg.fr/~maudin/analysecomp.pdf`.

[6] David J. BENSON : *Representations and cohomology. I*, volume 30 de *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, deuxième édition, 1998. Basic representation theory of finite groups and associative algebras.

[7] Garrett BIRKHOFF : *Lattice theory.* American Mathematical Society Colloquium Publications, vol. 25, revised edition. American Mathematical Society, New York, N. Y., 1948.

[8] Klaus BONGARTZ : Degenerations for representations of tame quivers. *Annales Scientifiques de l'E.N.S.*, 28(5):647–668, 1995. Disponible en ligne : `http://archive.numdam.org/ARCHIVE/ASENS/ASENS_1995_4_28_5/ASENS_1995_4_28_5_647_0/ASENS_1995_4_28_5_647_0.pdf`.

[9] Richard E. BORCHERDS : What is Moonshine? *In Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998)*, numéro Extra Vol. I, pages 607–615 (électronique), 1998.

*NDÉ. *À ne pas confondre (ou à confondre) avec le livre culte de Douglas Adams "HitchHiker's Guide to the Galaxy".*

[10] Nicolas BOURBAKI : *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV : Groupes de Coxeter et systèmes de Tits. Chapitre V : Groupes engendrés par des réflexions. Chapitre VI : systèmes de racines.* Actualités Scientifiques et Industrielles, No. 1337. Hermann, Paris, 1968.

[11] Jean-Pierre BOURGUIGNON : *Calcul variationnel.* Éditions de l'École polytechnique, Palaiseau, 2007.

[12] Maxime BOURRIGAN : Dobble et la géométrie finie. *Images des mathématiques, CNRS*, disponible en ligne : `http://images.math.cnrs.fr/Dobble-et-la-geometrie-finie.html`, 2011.

[13] Frédéric BRECHENMACHER : La controverse de 1874 entre Camille Jordan et Leopold Kronecker. *Rev. Histoire Math.*, 13(2):187–257, 2007.

[14] Josette CALAIS : *Éléments de théorie des groupes.* Presses universitaires de France, 1984.

[15] Arthur CAYLEY : On the theory of analytical forms called trees. *Philosophical Magazine*, 13:172–176, 1857. Réédité dans : *The Collected Mathematical Papers of Arthur Cayley.* Vol. 3, Cambridge University Press, Cambridge, 1890, p. 242-246 ; `http://archive.org/details/collmathpapers03caylrich`.

[16] Neil CHRISS et Victor GINZBURG : *Representation theory and complex geometry.* Modern Birkhäuser Classics. Birkhäuser Boston Inc., Boston, MA, 2010. Réimpression de l'édition de 1997.

[17] William CLIFFORD : A synthetic proof of Miquel's theorem. *Oxford, Cambridge and Dublin Messenger of Mathematics*, 5:124–141, 1870.

[18] H. S. M. COXETER : Self-dual configurations and regular graphs. *Bull. Amer. Math. Soc.*, 56:413–455, 1950.

[19] H. S. M. COXETER : *Introduction to geometry.* John Wiley & Sons Inc., New York, deuxième édition, 1969.

[20] Richard DEDEKIND : Ueber die von drei Moduln erzeugte Dualgruppe. *Math. Ann.*, 53(3):371–403, 1900.

[21] John D. DIXON et Brian MORTIMER : *Permutation groups*, volume 163 de *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996.

[22] John DOUGALL : An extension of Clifford's circle chain. *Mathematical Notes*, 26:i–v, 1930.

[23] Patrick DU VAL : On isolated singularities of surfaces which do not affect the conditions of adjunction. I, II, III. *Proc. Camb. Philos. Soc.*, 30:453–465, 483–491, 1934.

[24] Daniel DUVERNEY : *Théorie des nombres.* Collection Sciences Sup. Dunod, deuxième édition, 2007. Cours et exercices corrigés.

[25] Charles EHRESMANN : Sur la topologie de certains espaces homogènes. *Ann. of Math. (2)*, 35(2):396–443, 1934.

[26] Pavel ETINGOF, Oleg GOLBERG, Sebastian HENSEL, Tiankai LIU, Alex SCHWENDNER, Dmitry VAINTROB et Elena YUDOVINA : *Introduction to representation theory*, volume 59 de *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2011. Avec des interludes historiques par Slava Gerovitch.

[27] Jacques FARAUT : *Analyse sur les groupes de Lie*. Mathématiques en devenir. Calvage et Mounet, Paris, 2006. Une introduction.

[28] Ralph FREESE : Free modular lattices. *Trans. Amer. Math. Soc.*, 261(1):81–91, 1980.

[29] William FULTON : *Young tableaux*, volume 35 de *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1997. With applications to representation theory and geometry.

[30] William FULTON : *Intersection theory*, volume 2 de *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, deuxième édition, 1998.

[31] William FULTON et Joe HARRIS : *Representation theory*, volume 129 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[32] Sylvestre GALLOT, Dominique HULIN et Jacques LAFONTAINE : *Riemannian geometry*. Universitext. Springer-Verlag, Berlin, troisième édition, 2004.

[33] Meinolf GECK : *An introduction to algebraic geometry and algebraic groups*, volume 10 de *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2003.

[34] I. M. GEL'FAND et V. A. PONOMAREV : Remarks on the classification of a pair of commuting linear transformations in a finite-dimensional space. *Funkcional. Anal. i Priložen.*, 3(4): 81–82, 1969.

[35] I. M. GEL'FAND et V. A. PONOMAREV : Quadruples of subspaces of finite-dimensional vector space. *Dokl. Akad. Nauk SSSR*, 197:762–765, 1971.

[36] Gábor GÉVAY et Tomaž PISANSKI : Kronecker covers, V-construction, unit-distance graphs and isometric point-circle configurations. *Ars Math. Contemp.*, 7(2):317–336, 2014.

[37] Gérard GONZALEZ-SPRINBERG et Jean-Louis VERDIER : Construction géométrique de la correspondance de McKay. *Ann. Sci. École Norm. Sup. (4)*, 16(3):409–449 (1984), 1983.

[38] Branko GRÜNBAUM : *Configurations of points and lines*, volume 103 de *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009.

[39] Daniel GUIN : *Algèbre II, Anneaux, modules et algèbre multilinéaire*. Collection Enseignement sup. EDP Sciences, Grenoble, 2013.

[40] Roger HEATH-BROWN : Fermat's two squares theorem. *Invariant*, 11: 3–5, 1984. Disponible en ligne : `http://eprints.maths.ox.ac.uk/677/1/invariant.pdf`.

[41] Bruno INGRAO : *Coniques projectives, affines et métriques*. Mathématiques en devenir. Calvage et Mounet, Paris, 2011.

[42] Heinrich W. E. JUNG : Über ganze birationale Transformationen der Ebene. *J. Reine Angew. Math.*, 184:161–174, 1942.

[43] Victor G. KAC : Infinite root systems, representations of graphs and invariant theory. *Invent. Math.*, 56(1):57–92, 1980.

[44] Mikhail KAPRANOV et Éric VASSEROT : Kleinian singularities, derived categories and Hall algebras. *Math. Ann.*, 316(3):565–576, 2000.

[45] Alexandre A. KIRILLOV : *Éléments de la théorie des représentations*. Éditions Mir, Moscou, 1974. Traduit du russe par A. Sossinsky.

[46] Serge LANG : *Algèbre*. Science Sup. Dunod, Paris, 2004. Troisième édition, revue et augmentée. Cours et exercices.

[47] François LAUDENBACH : *Calcul différentiel et intégral*. Éditions de l'École polytechnique, Palaiseau, 2001.

[48] Ian G. MACDONALD : *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, deuxième édition, 1995. Avec des contributions d'A. Zelevinsky, Oxford Science Publications.

[49] Peter MAGYAR, Jerzy WEYMAN et Andrei ZELEVINSKY : Multiple flag varieties of finite type. *Adv. Math.*, 141(1):97–118, 1999.

[50] Aimeric MALTER, Dierk SCHLEICHER et Don ZAGIER : New looks at old number theory. *Amer. Math. Monthly*, 120(3):243–264, 2013.

[51] Laurent MANIVEL : *Fonctions symétriques, polynômes de Schubert et lieux de dégénérescence*, volume 3 de *Cours Spécialisés*. Société Mathématique de France, Paris, 1998.

[52] Olivier MATHIEU : Une formule sur les opérateurs différentiels en caractéristique non nulle. *C. R. Acad. Sci. Paris Sér. I Math.*, 304(14):405–406, 1987.

[53] John MCKAY : Graphs, singularities, and finite groups. *In The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 de *Proc. Sympos. Pure Math.*, pages 183–186. Amer. Math. Soc., Providence, R.I., 1980.

[54] John McKay : Cartan matrices, finite groups of quaternions, and Kleinian singularities. *Proc. Amer. Math. Soc.*, 81(1):153–154, 1981.

[55] Henry McKean et Victor Moll : *Elliptic curves.* Cambridge University Press, Cambridge, 1997. Function theory, geometry, arithmetic.

[56] Jean-Yves Mérindol : *Nombres et algèbre.* Collection Grenoble sciences. EDP-Sciences, Grenoble, 2006.

[57] Auguste Miquel : Sur les intersections des cercles et des sphères. *Journal de mathématiques pures et appliquées*, 3:517–522, 1838.

[58] Rached Mneimné : *Éléments de géométrie.* Nouvelle bibliothèque mathématique, 2. Cassini, Paris, 1997. Actions de groupes.

[59] Rached Mneimné : *Réduction des endomorphismes – Tableaux de Young, cône nilpotent, représentations des algèbres de Lie semi-simples.* Tableau noir. Calvage et Mounet, 2006.

[60] Rached Mneimné et Frédéric Testard : *Introduction à la théorie des groupes de Lie classiques.* Collection Méthodes. Hermann, Paris, 1986.

[61] Shigeru Mukai : *An introduction to invariants and moduli*, volume 81 de *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 2003. Traduit des éditions en japonais de 1998 et 2000 par W. M. Oxbury.

[62] Richard K. Oliver : On the parity of a permutation. *Amer. Math. Monthly*, 118(8):734–735, 2011.

[63] Frédéric Paulin : *Géométrie différentielle élémentaire*, 2007. Cours de première année de mastère à l'École normale supérieure, années 2003-2007, `http://www.math.u-psud.fr/~paulin/notescours/cours_geodiff.pdf`.

[64] Daniel Perrin : *Géométrie algébrique.* Savoirs actuels. InterEditions, Paris, 1995. Une introduction.

[65] Daniel Perrin : *Cours d'algèbre.* Collection CAPES/agrégation. Éditions Ellipses, Paris, 1997.

[66] Daniel Perrin : *Géométrie projective plane et applications aux géométries euclidienne et non euclidiennes.* En préparation, 2011. `http://www.math.u-psud.fr/~perrin/Livre_de_geometrie_projective.html`.

[67] Gabriel Peyré : *L'algèbre discrète de la transformée de Fourier.* Mathématiques à l'Université. Éditions Ellipses, Paris, 2004.

[68] Tomaž Pisanski et Brigitte Servatius : *Configurations from a graphical viewpoint.* Birkhäuser Advanced Texts : Basler Lehrbücher. Birkhäuser/Springer, New York, 2013.

[69] Paul PRÉAU : Un graphe ternaire associé à l'équation $X^2 + Y^2 = Z^2$. *C. R. Acad. Sci. Paris Sér. I Math.*, 319(7):665–668, 1994.

[70] Jean-Jaques RISLER et Pascal BOYER : *Algèbre pour la licence 3 - Groupes, anneaux, corps.* Dunod, Paris, 2006.

[71] Pierre SAMUEL : *Théorie algébrique des nombres.* Hermann, Paris, 1967.

[72] Ralf SCHIFFLER : *Quiver representations.* CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer-Verlag, New York, 2014.

[73] Clément de SEGUINS-PAZZIS : *Invitation aux formes quadratiques.* Mathématiques en devenir. Calvage et Mounet, Paris, 2011.

[74] Denis SERRE : *Les matrices. Théorie et pratique.* Masson sciences. Dunod, Paris, 2001.

[75] Jean-Pierre SERRE : *Cours d'arithmétique.* Presses Universitaires de France, Paris, 1977. Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[76] Jean-Pierre SERRE : *Représentations linéaires des groupes finis.* Hermann, Paris, deuxième édition, 1978.

[77] Ivan P. SHESTAKOV et Ualbai U. UMIRBAEV : The Nagata automorphism is wild. *Proc. Natl. Acad. Sci. USA*, 100(22):12561–12563, 2003.

[78] Peter SLODOWY : *Simple singularities and simple algebraic groups*, volume 815 de *Lecture Notes in Mathematics.* Springer, Berlin, 1980.

[79] Richard P. STANLEY : *Enumerative combinatorics. Vol. 2*, volume 62 de *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.

[80] Michio SUZUKI : *Group theory. I*, volume 247 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1982. Traduit du japonais par l'auteur.

[81] Lajos SZILASSI : Les toroïdes réguliers. *Structural Topology*, (13):69–80, 1986. Dual French-English text.

[82] Wouter van der KULK : On polynomial rings in two variables. *Nieuw Arch. Wiskunde (3)*, 1:33–41, 1953.

[83] André WEIL : Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

[84] Don ZAGIER : A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. *Amer. Math. Monthly*, 97(2):144, 1990.

[85] Andrei ZELEVINSKY : What is... a cluster algebra? *Notices Amer. Math. Soc.*, 54(11):1494–1495, 2007.

Index

action
    par automorphismes, 404
    sur un graphe, 513
    par tensorisation, 492
algèbre
    extérieure, 65
    des fonctions polynomiales, 404
    graduée, 497
    de Hall, 222
    de Hecke, 39
    de Lie, 138, 291
analogue quantique, 195
anisotrope, 206
arbre enraciné, 260
autopolaire
    triangle —, 238

base
    orthonormée symplectique, 296
    symplectique, 293
birapport, 157
BN-paire, 37
bord, 175
Borel
    sous-groupe de —, 31
boucle, 135
Bruhat
    décomposition de —, 26
    ordre de —, 28, 49

caractère, 453
    irréductible, 453
carquois, 135
carré
    alterné, 462, 463
    symétrique, 462, 463
cellule de Schubert, 27
centrale
    fonction —, 455
cercle hyperbolique, 350
chemin, 165
    paresseux, 165
coadjointe
    orbite —, 332
coefficient binomial quantique, 195
cohomologie galoisienne, 219
coloriage, 250
composable, 165
composante isotypique, 451
composition, 161
condition d'échange, 50
configuration
    autoduale, 230
    de Cremona-Richmond, 244, 287
    duale, 230
    groupe d'une —, 229
    indécomposable, 113
    isomorphisme de —s, 229
    morphisme de —s, 113
    de points, 229
    de sous-espaces, 113
conique affine, 387
conjectures de Weil, 213
conjugué harmonique, 378
conoyau, 139
coordonnées homogènes, 10
courbe elliptique, 340
cycle, 174
cyclique
    espace —, 78

décimation, 50
décomposition
    de Bruhat, 26
    polaire, 301
déformation quantique, 43
Demazure
    désingularisation de —, 71
désingularisation de Demazure, 71
développement par blocs, 4
distance
    de Hilbert, 349
    hyperbolique, 347

Dobble, 265
drapeau
complet, 20
de la configuration, 230
standard, 20
variété des —x, 21
droite
extérieure, 270
polaire, 238, 271
sécante, 270
tangente, 269

éclatement, 543
Ehresmann
ordre d'—, 51
énigmatique inéquation, 176
équation
de Pell-Fermat, 387
équianharmonique, 369
espace
des bords, 140
des cycles, 140
cyclique, 78
des extensions, 140, 175
gradué, 497
des représentations, 143
simple, 79
exacte
suite —, 140
extension, 140, 174
extensions équivalentes, 141, 175

facteurs invariants, 79, 99
factorielle quantique, 195
faisceau de cercles, 316
fini
carquois —, 135
carquois de type —, 155
Fitting
lemme de —, 168
flèche, 135
fonction
centrale, 455
de Schur, 268
forme
G-invariante, 482
homologique, 139
symplectique, 292
de Tits, 150
formule
de Binet-Cauchy, 2
de Burnside, 414
de Burnside pondérée, 255
de Laplace, 2
Frobenius
indicateur de — -Schur, 482
réciprocité de —, 552

graphe
de Cayley, 366
de McKay, 513
de Paley, 283
grassmannienne, 20
groupe
$\mathfrak{A}_4$, 252, 422, 430, 520, 566
$\tilde{\mathfrak{A}}_4$, 520
$\mathfrak{A}_5$, 244, 378, 423, 433, 525, 565
$\tilde{\mathfrak{A}}_5$, 525
binaire, 508
diédral, 511, 515
icosaédral, 525
octaédral, 522
tétraédral, 520
de Borel, 31
d'une configuration, 229
diédral, 56, 554
de Klein, 337
libre, 55
de Lie, 143
$\mathrm{PSL}_2(\mathbb{F}_7)$, 72, 265, 284, 369, 379, 554, 565, 566
$\mathfrak{S}_4$, 230, 337, 377, 422, 432, 522, 566
$\tilde{\mathfrak{S}}_4$, 522
$\mathfrak{S}_5$, 244, 378
$\mathfrak{S}_6$, 73, 244, 288, 560
symplectique, 293
unipotent, 31

Hall
algèbre de —, 222
harmonique, 369

Hecke
algèbre de —, 39
homogène, 11
horocycle, 351, 352

idempotent, 166
indécomposable
module —, 93
indicateur
de Frobenius-Schur, 482
indice de Witt, 206
invariant
anallagmatique, 319
de similitude, 79
modulaire, 340
inversion, 47
nombre d'—s, 47
irréductible
caractère —, 453
module —, 93
représentation —, 136, 443
isotrope, 206
Iwahori-Hecke
algèbre d'—, 39

Jordan-Kronecker
théorème de —, 125

Klein
correspondance de —, 307
groupe de —, 337

lagrangien, 219, 330
lemme
de Fitting, 168
de Schur, 447
local
anneau —, 169
longueur
d'un chemin, 165
d'une permutation, 40, 46

matrice
compagnon, 99, 214
de Pauli, 509
de permutation, 26

McKay
graphe de —, 513
module, 92, 94
indécomposable, 93
irréductible, 93
morphisme de —s, 93
projectif, 186
quotient, 93, 95
simple, 93
somme directe de —s, 93
sous- —, 92
Molien
série de —, 500
morphisme
de modules, 93
de représentations, 136, 443
multiplicité, 451

nombre
d'inversions, 4
pentagonal, 200

ordre
de Bruhat, 28, 49
de dégénérescence, 29, 146
d'Ehresmann, 51
ext, 147
hom, 147

parabolique
sous-groupe —, 35
parabolique minimal
sous-groupe —, 35
parfait
corps —, 81
pfaffien, 308, 328
ping-pong, 362
plan
de Fano, 265, 283
hyperbolique, 357
plongement
de Plücker, 8
de Segre, 307
de Veronese, 305
Plücker
plongement de —, 8
relations de —, 10

point
— bases, 317, 346
entier, 387
extérieur, 235, 269
intérieur, 235, 269
— limites, 317, 346
rationnel, 387
polaire (d'un point), 238, 271
pôle
(d'une droite), 271
(d'une rotation), 414
polynôme
générateur, 252
indicateur de cycles, 252
de Newton, 254
poset, 54
position w, 70
poussée en avant, 150, 173
présentation, 42
par générateurs et relations, 56
problème du mot, 133
produit
tensoriel, 540
propriété
universelle, 55
puissance tensorielle, 542
pullback, 150, 172
pushforward, 150, 173

quantique
analogue —, 195
coefficient binomial —, 195
factorielle —, 195
quotient
module —, 93, 95
représentation —, 136, 445

racine
d'un arbre, 260
positive, 153
réciprocité de Frobenius, 552
relations
de Plücker, 10
de Ptolémée, 10
représentation
d'un carquois, 136
complexe, 482
degré d'une —, 443
fidèle, 443
fondamentale, 6
indécomposable, 136
induite, 268, 549
irréductible, 136, 443
isomorphisme de —s, 136
linéaire d'un groupe, 443
matricielle, 446
morphisme de —s, 136
par permutation, 458
quaternionique, 482
quotient, 136, 445
réelle, 482
régulière, 444, 466
semi-simple, 448
simple, 136, 443
somme directe de —s, 136
de Steinberg, 558
triviale, 444
vecteur de dimension d'une —, 139
représentations
isomorphisme de —, 443
morphisme de —, 443
somme directe de —, 444

sauvage, 123
Schubert
cellule de —, 27
variété de —, 33
Schur
indicateur de Frobenius- —, 482
lemme de —, 447
scindé, 142
semi-homographie, 232
semi-linéaire, 232
série
formelle, 223
génératrice, 198, 497
de Molien, 500
SETI, 206
SETIM, 206
signature
(d'un sous-groupe fini de SO(3)), 415

simple
endomorphisme —, 79
espace —, 79
module —, 93
représentation —, 136, 443
transposition —, 33
simplexe, 420
somme directe
de modules, 93
de représentations, 136, 444
sommet, 135
source, 165
sous-espace
totalement isotrope, 206
totalement isotrope maximal, 206
sous-expression, 50
sous-module, 92
sous-représentation, 136, 443
structure
conforme, 353
symplectique, 293
subimmersion, 143
suite exacte, 140
système
de Tits, 37
de relations, 55
symplectique, 294

table des caractères, 469
tableau, 51
terminus, 165
théorème
de décomposition de Frobenius, 79
de Gabriel, 153
de Jordan-Kronecker, 125
de Kac, 157
de Krull-Schmidt, 170
de Maschke, 448
des nombres pentagonaux d'Euler, 200
de Pascal, 393
de Pólya, 254
tirée en arrière, 150, 172
Tits
forme de —, 150
système de —, 37
tore
déployé, 274
non déployé, 274
transposition simple, 33
triangle
autopolaire, 238
équilatéral, 370
triple produit de Jacobi, 198
triplet pythagoricien, 363
primitif, 363
type
docile, 133
d'un drapeau, 27
Dynkin, 176
Dynkin affine, 179
fini, 133
sauvage, 134
d'un sous-espace, 21

unipotent, 31

variété
de Bott-Samelson, 71
des drapeaux, 21
d'incidence, 64
de Schubert, 33
vecteur de dimension, 139

Imprimé en Belgique et achevé sur les presses de SNEL Grafics, à Liège
Dépôt légal mars 2015

Le présent livre est le dernier volet, tant attendu, des « contes hédonistes », que nous retracent avec magie Philippe Caldero et Jérôme Germoni. Les lecteurs y sont transportés, comme sur un tapis volant, dans un parcours contemplatif et raisonné des interactions entre groupes et géométries. Nos deux capitaines ne réclament à leurs passagers aucun document de voyage, mais un simple bagage mathématique de niveau master.

Ce second volume suit le même canevas que son prédécesseur, en proposant de nombreux thèmes où les groupes jouent un rôle déterminant. Une place de choix est accordée à la théorie des représentations, qui fait désormais partie du programme de l'agrégation. Mais au-delà du cadre restrictif des programmes de concours, on découvrira quelques morceaux de bravoure, comme deux études topologiques des grassmanniennes, l'une élémentaire et l'autre à l'aide des coordonnées de Plücker, ou un survol de la théorie des carquois de Peter Gabriel. On y rencontre aussi la féconde théorie de McKay. Une des vocations de ce volume est, après tout, de pourvoir quelques outils de la recherche actuelle à l'intention des étudiants en master ou des professeurs du supérieur.

Des solides platoniciens aux grassmanniennes, en passant par quelques territoires défrichés naguère par cet autre magicien que fut Harold Scott Coxeter, les lecteurs comprendront combien la géométrie a été et reste la source d'inspiration première de toutes ces belles mathématiques. Ils saisiront également comment la théorie des groupes est là pour donner du recul à l'apprenti mathématicien et l'aider à sortir de sa caverne de Platon.

Jérôme Germoni est ancien élève de l'ÉNS et maître de conférences à l'université Lyon 1. Il a été directeur de l'IREM de Lyon et préside actuellement la Maison des mathématiques et de l'informatique (MMI).

Philippe Caldero est maître de conférences à l'université Lyon 1 et ancien élève de l'ÉNS de Saint-Cloud. Plusieurs fois membre du jury de l'agrégation externe, il est très impliqué dans la préparation à l'agrégation interne, comme responsable et comme enseignant.

Collection.– Mathématiques en devenir

ISBN 978-2-91-635243-5

Calvage & Mounet

www.calvage-et-mounet.fr

Prix : 47 €